



The Open
University

M303

Further pure mathematics

Book A

Number theory

This publication forms part of the Open University module M303 *Further pure mathematics*. Details of this and other Open University modules can be obtained from Student Recruitment, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)300 303 5303; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2014. Second edition 2016.

Copyright © 2014, 2016 The Open University

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS (website www.cla.co.uk).

Open University materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or retransmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University T_EX System.

Printed in the United Kingdom by Halstan & Co. Ltd, Amersham, Bucks.

ISBN 978 1 4730 2036 8

2.1

Contents

Chapter 1	Foundations	1
Introduction		3
1	What is number theory?	4
2	Numbers from patterns	6
2.1	Polygonal numbers	7
2.2	Pyramidal numbers	12
3	Mathematical induction	15
3.1	Notation	15
3.2	Mathematical induction	16
3.3	More general induction	20
4	Divisibility	27
4.1	Integer division	27
4.2	The highest common factor	31
4.3	The least common multiple	38
5	Linear Diophantine equations	40
5.1	The Euclidean Algorithm	41
5.2	Linear Diophantine equations	44
Learning outcomes		49
Solutions to exercises		50

Chapter 2	Prime numbers	67
	Introduction	69
1	The primes	70
1.1	Basic properties	70
1.2	The sieve of Eratosthenes	72
1.3	The Fundamental Theorem of Arithmetic	74
2	The prime decomposition of integers	79
2.1	The prime decomposition of factors	79
2.2	The τ function	81
3	The infinitude of the primes	83
3.1	Euclid's Theorem	83
3.2	Primes in arithmetic progression	86
3.3	Primes generated by polynomials	90
4	Famous problems concerning primes	94
4.1	Proximity of primes	94
4.2	The Goldbach Conjecture	96
4.3	The Prime Number Theorem	97
5	Fibonacci numbers	100
5.1	The Fibonacci sequence	100
5.2	Properties of Fibonacci numbers	103
	Learning outcomes	108
	Solutions to exercises	109
	Appendix: Table of primes	122

Chapter 3	Congruence	125
Introduction		127
1	Properties of congruence	127
1.1	Definition and basic properties	128
1.2	Residue classes	132
1.3	Further properties	136
2	Divisibility tests	140
3	Linear congruences	144
3.1	Polynomial congruences	144
3.2	Linear congruences	146
3.3	Solving linear congruences	148
4	Simultaneous linear congruences	152
4.1	The Chinese Remainder Theorem	152
4.2	Solving simultaneous congruences	156
Learning outcomes		161
Solutions to exercises		162

Chapter 4	Fermat's and Wilson's Theorems	177
	Introduction	179
1	Fermat's Little Theorem	180
1.1	Statement and proof of Fermat's Little Theorem	181
1.2	Pseudoprimes	184
2	Representation of fractions by decimals	186
2.1	Terminating and cycling decimals	186
2.2	The order of an integer	189
2.3	Decimal representations of rational numbers	192
3	Wilson's Theorem	195
4	Polynomial congruences	199
4.1	Lagrange's Theorem	199
4.2	Factorising polynomial congruences	202
4.3	Congruences with composite moduli	207
5	Fermat's and Wilson's Theorems revisited	210
	Learning outcomes	214
	Solutions to exercises	215
	Index	229

Chapter 1

Foundations

Introduction

Welcome to Book A *Number theory*. This first chapter lays a firm foundation for the number theory components of the module. It examines in detail the fundamental ideas that form the basis from which to study the properties of numbers. We introduce, and make precise, the key notion of *divisibility*. For this we use a result concerning the division of one integer by another, which will be familiar to you. This result is known as the *Division Algorithm*. Its consequences, both practical and theoretical, make it a cornerstone of number theory. Through it we embark on a study of the properties of divisibility, and introduce the concept of the *highest common factor* – a topic that might already be familiar to you and one that is going to figure prominently in this part of the module. The chapter also reviews a powerful method of proof in number theory: *proof by mathematical induction*. You may well have met this idea before, but it is of such importance to us that we give a complete treatment here.

Before we get down to any theoretical ideas we need some families of numbers to which we might apply our techniques, and that is where we begin, after first giving a brief preview in Section 1 of some of the tasks that will confront us in the module.

Chapter guide

Section 1 gives a brief introduction to the kinds of problem that arise in number theory, which should require little study time. You may have seen aspects of the material in Sections 2 and 5 in other modules that you have studied, but here we take a more rigorous approach. The main focus of this chapter is on mathematical induction, covered in Section 3, and on the notion of divisibility, covered in Section 4. Section 5 introduces linear Diophantine equations, a topic that you will encounter again in Book C.

1 What is number theory?

The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes of reasoning it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and ten times more entertaining as the same amount of 'calculus for engineers'.

G.H. Hardy, *Bulletin of the AMS* (1929)

There is an irresistible fascination in searching for numbers with specified properties. Nearly every century, as far back as the history of mathematics can be traced, has witnessed new and exciting discoveries concerning properties of numbers. Many of the greatest mathematicians, despite having their major interests elsewhere, have at some time in their careers been drawn into problems of number theory and have contributed to the body of knowledge. So what is the appeal of this subject both for professional mathematicians and for thousands of amateurs?

Consider the following problems.

1. Find all the factors of 4 294 967 297.
2. A right-angled triangle has the property that all three of its sides have length equal to a whole number of units. If one of the sides is 24, find seven pairs of values for the other two sides.
3. Show that

$$1 \times 2 \times 3 \times 4 \times \cdots \times (n-1) + 1$$
 is always divisible by n if n is prime, but is never divisible by n if n is composite.
4. Can every even integer from 4 onwards be expressed as the sum of two primes?
5. For which integers n is $2^n - 1$ a prime?

All these problems will confront us at some stage in this part of the module. Each one illustrates the most attractive feature of number theory: the problems can be understood by beginners of the subject. Perhaps you are not completely familiar with some of the terms (which will be explained later) such as prime, composite and factor, but you should have a feeling for what is involved in these problems. Indeed, you could well take pencil and paper and start exploring some of them; there is no substantial body of knowledge needed as a prerequisite to becoming involved in number theory.

Yet while there is no difficulty posing these problems in a readily intelligible form, the varying degrees of difficulty involved in solving them highlights the most intriguing feature of number theory.

Because of the size of the number involved, Problem 1 is quite tricky. However, any reader who is familiar with computers might quickly solve this problem. As it happens, the smallest positive factor of the given number is 641 – a fact which, in the seventeenth century, eluded one of the all-time great mathematicians, Fermat (1601–1665), who had a particular interest in this very problem.

Problem 2 asks for solutions in whole numbers of the famous equation of Pythagoras relating the edge lengths of a right-angled triangle, $x^2 + y^2 = z^2$ (illustrated in Figure 1.1). This is an example of a Diophantine equation, named after the Greek mathematician Diophantus of the early Christian era. We will meet other instances of Diophantine equations in this module, which we will show how to solve. Many books have been written about Diophantine equations. What emerges is a lack of a general theory for solving them; each Diophantine equation appears to be a problem in its own right, requiring its own method of solution. In the meantime, if you are familiar with the ‘smallest’ solution in integers of the Pythagorean equation, namely $3^2 + 4^2 = 5^2$, then you may have spotted two of the solutions required by Problem 2 by scaling, namely $18^2 + 24^2 = 30^2$ and $24^2 + 32^2 = 40^2$. But what about the other five solutions? You might discover them by patient trial and error – but is there a more systematic approach? We will explore this further at the start of Book C, Chapter 12.

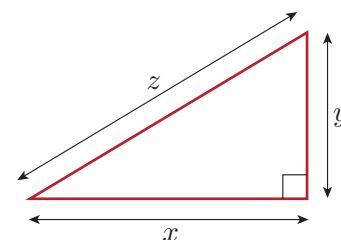


Figure 1.1 An illustration of the Pythagorean equation $x^2 + y^2 = z^2$

Problems 3, 4 and 5 are classics of number theory. Because the values involved in Problem 3 get very large, very quickly, it is not an easy problem to explore in depth by looking at special cases. But it turns out to be true, and we can give (and will do so in Chapter 4) a general proof of this result. Problem 4 is easier to explore and, on finding it very straightforward to write each even integer up to 200 (say) as a sum of two primes, you would probably be tempted to conclude that it also is a true result. But, perhaps surprisingly, nobody has ever managed to prove it; to this day it remains an unsolved problem of mathematics, despite assault by many great mathematicians. Problem 5 has its origin at the heart of another famous problem, which you will meet in Book C, Chapter 9. By the year 1951, only 12 numbers n were known for which $2^n - 1$ is prime; then computers were brought to bear on the problem, with the result that by the year 2014 forty-eight such numbers were known. The largest one, $n = 57\,885\,161$, led to the number $2^{57\,885\,161} - 1$ being the largest known prime at that time. And yet, despite the scarcity of solutions to Problem 5, most mathematicians still believe that there are infinitely many solutions to this problem – though proof of this seems, at the moment, hopelessly beyond reach.

Number theory is a subject that has developed over a long period of time and, as the previous paragraph suggests, remains very active today. We have already mentioned a few of the great mathematicians who contributed to the development of the subject; there are many, many more. In the *History Reader* for this topic, we give a flavour of the history of the subject. The *History Reader* is not an assessed part of the module and by no means gives a systematic account of the history of number theory. Its inclusion will, we hope, enliven the theoretical side of the material and should also reveal the stumbling way in which progress has been made.

The nature of number theory has changed dramatically in recent years, due to the advent of the computer. Computations that were nigh impossible just a few years ago can now be managed with ease. Consequently, exploration of alleged results and searches for numbers with prescribed properties are readily attacked with the assistance of a machine. Although the material of this module presents many challenges for those with access to (and enthusiasm for) a computer, we have written the module in such a way as to avoid the heavy computational side of the subject. We will be attacking problems in the way that they have been tackled historically, using pencil and paper. There are, however, many problems in the module involving ‘arithmetic’ that could be simplified with the help of a calculator, and although it is not essential, it is advisable that you have one.

Number theory is all about problem-solving. Nobody becomes competent at calculus by reading about it; it is essential to practise differentiation and integration on a large number of examples. The same is true of number theory; you cannot get to grips with the subject without solving lots of problems yourself. To this end we have included a good stock of problems in all the chapters, and while studying you should always have pencil and paper at hand. The Worked Exercises in the chapters are for you to read, but the Exercises are for you to *do*. Do not spend forever on an exercise that looks like defeating you. If you get stuck, you should refer to the solution – but do not give in too easily!

2 Numbers from patterns

In this section we are concerned with certain families of numbers that can be derived from patterns, namely the polygonal numbers and the pyramidal numbers.

2.1 Polygonal numbers

Figure 2.1 illustrates the first five of the so-called **triangular numbers**, T_n . The arrangement of T_4 will be familiar to anyone who indulges in ten-pin bowling and T_5 is, more or less, the arrangement of the pack of 15 red balls at the start of a game of snooker. It is evident that the triangular numbers are the sums of consecutive integers starting from 1: $T_1 = 1$, $T_2 = 1 + 2$, $T_3 = 1 + 2 + 3$, $\dots$, $T_n = 1 + 2 + 3 + \dots + n$.

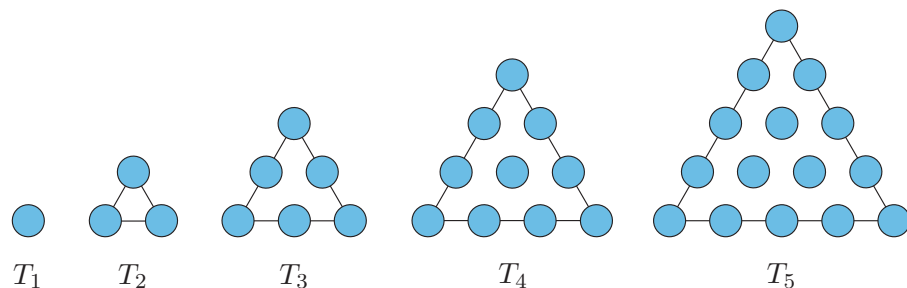


Figure 2.1 Triangular numbers

We can obtain a simple formula for T_n by writing the sum both forwards and backwards:

$$\begin{aligned} T_n &= 1 + 2 + 3 + \dots + n \\ T_n &= n + (n-1) + (n-2) + \dots + 1 \end{aligned}$$

and adding the two sums by pairing each term in the first line with the term directly below it. Each corresponding pair has a sum of $(n+1)$, so we obtain

$$2T_n = (n+1) + (n+1) + \dots + (n+1) = n(n+1),$$

giving

$$T_n = 1 + 2 + 3 + \dots + n = \frac{1}{2}n(n+1).$$

This same argument can be used for any arithmetic series. An **arithmetic series** is the sum of a finite sequence of terms in which the difference between consecutive terms is constant. So the arithmetic series having n terms with first term a and common difference d is

$$a + (a+d) + (a+2d) + \dots + (a+(n-1)d).$$

The sequence (rather than the sum) of terms

$$a, a+d, a+2d, \dots$$

is called an **arithmetic progression** (or arithmetic sequence). For example, the sequence of triangular numbers is an arithmetic progression with $a = d = 1$.

A formula for the arithmetic series can be obtained by reversing the sum and adding corresponding terms, as was done for the triangular numbers: each pair of corresponding terms sums to $2a + (n - 1)d$, and so we have

$$a + (a + d) + (a + 2d) + \cdots + (a + (n - 1)d) = \frac{1}{2}n(2a + (n - 1)d).$$

This formula can be rewritten as

$$n(a + \frac{1}{2}(n - 1)d),$$

illustrating that there are n terms of average $a + \frac{1}{2}(n - 1)d$.

Exercise 2.1

Determine the following sums.

(a) $3 + 10 + 17 + 24 + \cdots + 143$

(b) $100 + 98 + 96 + \cdots + 50$

Figure 2.2 shows that two consecutive triangular numbers add up to a **square number**, that is, a number of the form n^2 for some integer $n \geq 1$. In Figure 2.2, each square of dots is made up of a triangle of white dots and the next larger triangle of blue dots. Interpreting this observation in terms of triangular and square numbers, it would appear that

$$T_{n-1} + T_n = n^2, \quad n \geq 1.$$

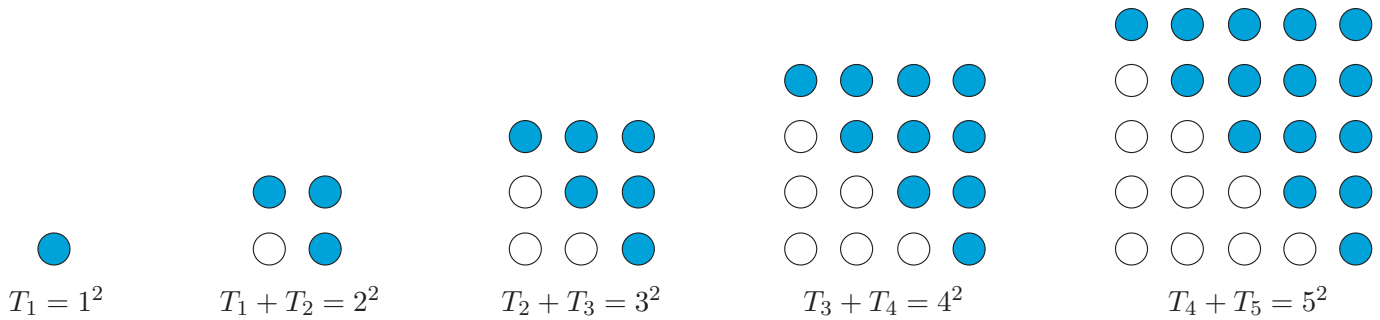


Figure 2.2 Adding consecutive triangular numbers

By convention we take $T_0 = 0$, which is the value given by the formula $\frac{1}{2}n(n + 1)$. A formal proof that $T_{n-1} + T_n$ is equal to n^2 is readily obtained using the formula for T_n :

$$T_{n-1} + T_n = \frac{1}{2}(n - 1)n + \frac{1}{2}n(n + 1) = \frac{1}{2}n(n - 1 + n + 1) = n^2.$$

In future we may refer to the square numbers merely as the squares. Square numbers are sometimes called perfect squares. Furthermore, we may shorten the phrase ‘is a triangular number’ to ‘is triangular’.

Exercise 2.2

- (a) You have seen that the triangular numbers are precisely the numbers of the form $\frac{1}{2}n(n+1)$. Show that if k is a triangular number then so is $9k+1$.
- (b) Show that an integer k is triangular if, and only if, $8k+1$ is square.

Note that since this is an ‘if, and only if’ statement, its proof will need to have two parts. You will need to show that if k is triangular then $8k+1$ is square and, conversely, that if $8k+1$ is square then k is triangular.

Hint: for the latter, note that the square number $8k+1$ is odd, and so it has to be the square of an odd number, that is, $8k+1 = (2s+1)^2$, for some integer s .

Let us reconsider the hint given in Exercise 2.2(b). It advised you to make use of the fact that you were dealing with an odd number. The odd integers

$$\dots, -3, -1, 1, 3, 5, \dots$$

are those that can be written as $2m+1$, for some integer m . The even integers

$$\dots, -4, -2, 0, 2, 4, \dots$$

are those that can be written as $2m$, for some integer m . Hence all integers can be written as a multiple of 2 plus a remainder r that is either 0 or 1. Expressing an integer as a multiple of a positive integer k plus a remainder r (where $0 \leq r < k$) can be a useful approach, as you will see in Section 4.

One instance of the result of Exercise 2.2(b) is illustrated in Figure 2.3. A 9×9 square of dots is broken into eight copies of $T_4 = 10$ with one dot left over in the middle.

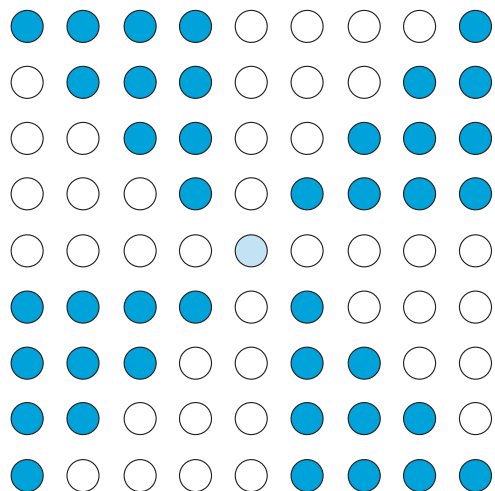


Figure 2.3 An illustration of $8T_4 + 1 = 9^2$

While the triangular numbers are sums of consecutive integers,

$$1, 1 + 2, 1 + 2 + 3, \dots,$$

Figure 2.4 illustrates that the squares are sums of consecutive odd integers,

$$1, 1 + 3, 1 + 3 + 5, \dots;$$

the next odd number is added to the current square as dots along the bottom and right-hand side to produce the next square.

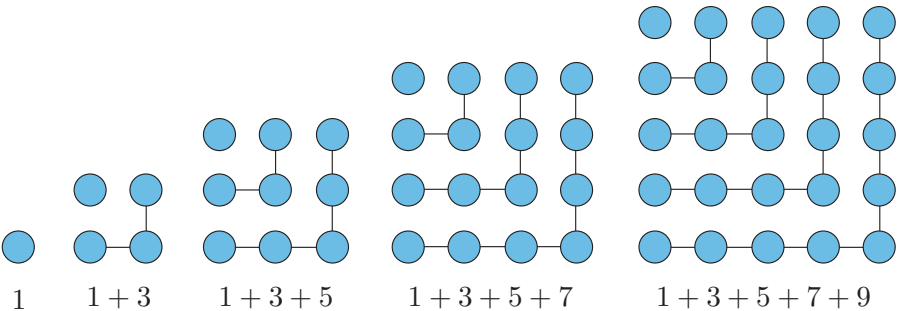


Figure 2.4 Squares as sums of odd integers

The general formula suggested by this sequence of diagrams is

$$1 + 3 + 5 + \dots + (2n - 1) = n^2, \quad n \geq 1.$$

A proof of this result is immediate from the formula for an arithmetic series but we will leave it aside for the time being. Formulas like this, in which results are asserted for each positive integer n , are often tailor-made for proof by the method of mathematical induction, which we deal with in Section 3.

Higher polygonal numbers

We have seen that triangular numbers are sums of consecutive integers, and squares are sums of consecutive odd integers. The pattern can be continued: **pentagonal numbers** are the sums obtained from going up in threes, namely

$$1, 1 + 4, 1 + 4 + 7, 1 + 4 + 7 + 10, \dots$$

Figure 2.5 illustrates the start of the sequence of pentagonal numbers, and Figure 2.6 goes one stage further and shows how the **hexagonal numbers**,

$$1, 1 + 5, 1 + 5 + 9, 1 + 5 + 9 + 13, \dots,$$

arise from arrangements of dots forming hexagons.

We will use ‘formulas’ rather than ‘formulae’ as the plural of ‘formula’.

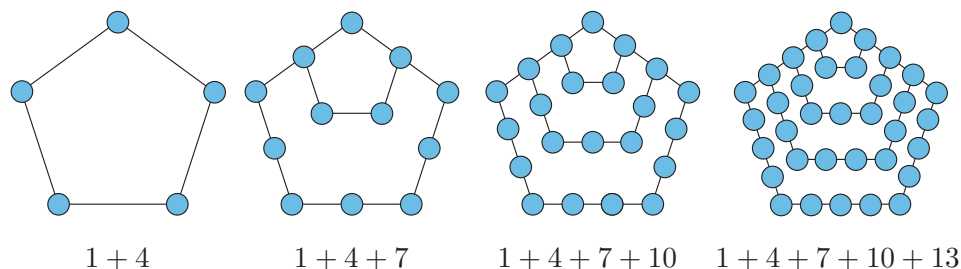
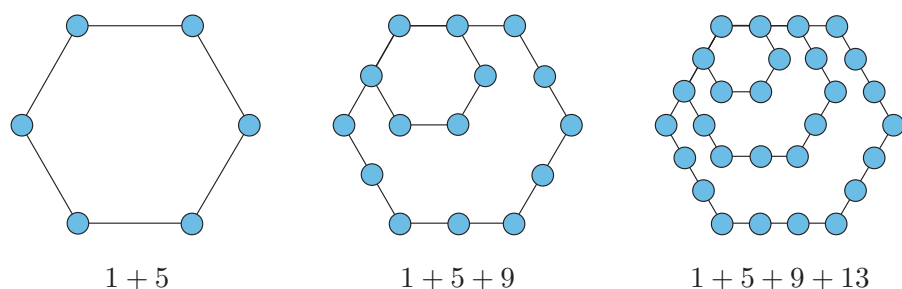
**Figure 2.5** Pentagonal numbers**Figure 2.6** Hexagonal numbers

Table 2.1 shows the beginnings of the sequences of **polygonal numbers**. The first row is the sequence of triangular numbers,

$$1, 1 + 2 = 3, 1 + 2 + 3 = 6, 1 + 2 + 3 + 4 = 10, \dots$$

We have extended the table beyond the numbers already seen by appealing to the emerging patterns. For example, the **octagonal numbers** form the sequence

$$1, 1 + 7, 1 + 7 + 13, 1 + 7 + 13 + 19, \dots$$

Table 2.1 Table of polygonal numbers

	Number of sides	Term 1	Term 2	Term 3	Term 4	Term 5	Term 6	Term 7	Term 8	...	Term n
Triangular	3	1	3	6	10	15	21	28	36	...	$\frac{1}{2}n(n+1)$
Square	4	1	4	9	16	25	36	49	64	...	n^2
Pentagonal	5	1	5	12	22	35	51	70	92	...	?
Hexagonal	6	1	6	15	28	45	66	91	120	...	?
Heptagonal	7	1	7	18	34	55	81	112	148	...	?
Octagonal	8	1	8	21	40	65	96	133	176	...	?
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k -gonal	k	1	k	$3k - 3$	?	?	?	?	?	...	$P(k, n)$

In the right-hand column we have listed the discovered formulas for the n th triangular number and for the n th square. The rest are missing, but could be determined from the appropriate arithmetic series. Along the bottom row we have begun listing the terms for the k -gonal numbers. You may be able to spot formulas (in terms of k) for these numbers from the patterns that are present in the table.

Of course, we could readily fill in the right-hand column and the bottom row if we could find a general formula for the n th term in the sequence of k -gonal numbers, which we will call $P(k, n)$. The next exercise invites you to provide this formula. Remember that $P(3, n)$, the n th triangular number, is the sum of n terms of the arithmetic progression with first term 1 and common difference 1; $P(4, n)$, the n th square, is the sum of n terms of the arithmetic progression with first term 1 and common difference 2; and, in general, $P(k, n)$ is the sum of n terms of the arithmetic progression with first term 1 and common difference $k - 2$.

Exercise 2.3

- (a) Obtain a formula for $P(k, n)$, the n th k -gonal number, and hence fill in the missing entries in Table 2.1.
- (b) The numbers in each of the columns of Table 2.1 appear to be in arithmetic progression. The common difference between two successive terms in each column is equal to the triangular number at the head of the previous column. That is,

$$P(k, n) = P(k - 1, n) + P(3, n - 1).$$

Prove this formula algebraically.

2.2 Pyramidal numbers

The polygonal numbers arise as sums of arithmetic progressions with first term 1. We can take this a stage further: the **pyramidal numbers** are those that arise as sums of finite sequences of polygonal numbers. For instance, from the sequence of triangular numbers,

$$1, 3, 6, 10, 15, \dots,$$

we obtain the **triangle-based pyramidal numbers** as follows:

$$1, 1 + 3 = 4, 1 + 3 + 6 = 10, 1 + 3 + 6 + 10 = 20, \dots$$

Figure 2.7 illustrates how these numbers arise from layers of a triangle-based pyramid.

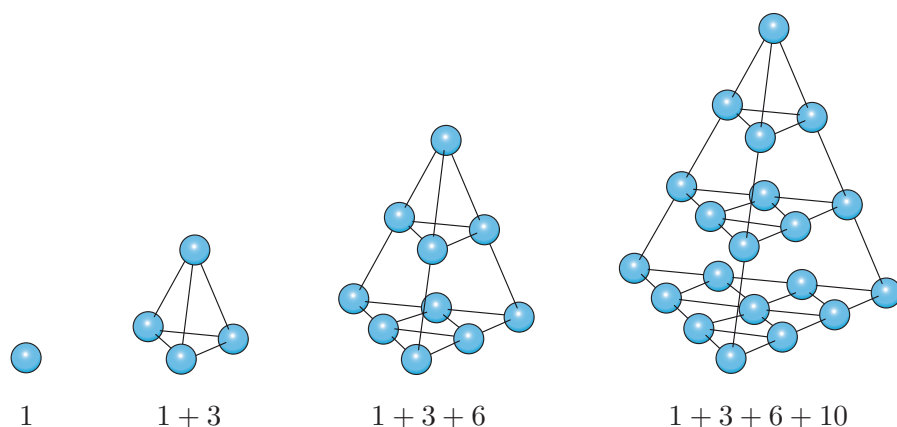


Figure 2.7 Triangle-based pyramidal numbers

Similarly, by adding consecutive terms of the sequence of squares we get the **square-based pyramidal numbers**

$$1, 1 + 4 = 5, 1 + 4 + 9 = 14, 1 + 4 + 9 + 16 = 30, \dots,$$

illustrated in Figure 2.8.

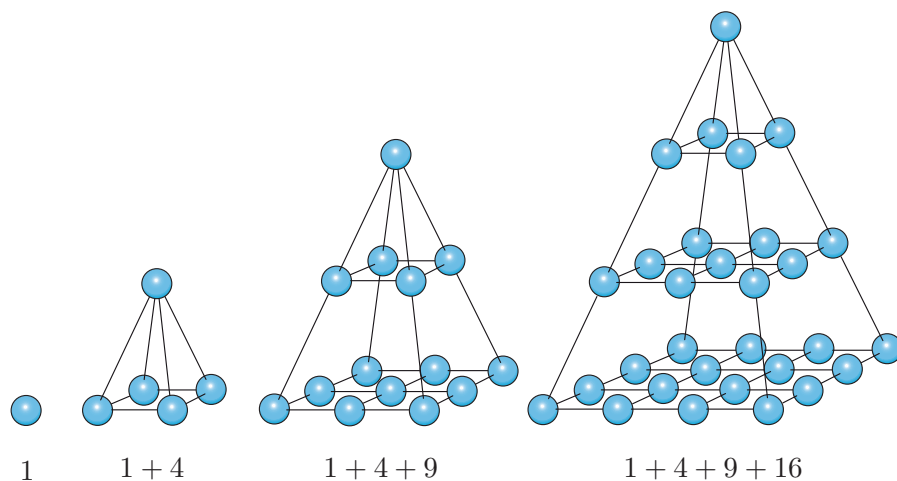


Figure 2.8 Square-based pyramidal numbers

The pyramidal numbers are readily generalised. For example, the **heptagonal-based pyramidal numbers** are generated as sums of heptagonal numbers,

$$1, 1 + 7 = 8, 1 + 7 + 18 = 26, 1 + 7 + 18 + 34 = 60, \dots$$

Table 2.2 gives some of the pyramidal numbers. We have started, but not completed, the row for the general k -gon and the column for the general n th term. The formulas that occur in the latter are not so easily proved; we return to them when we have discussed proof by mathematical induction.

Table 2.2 Table of pyramidal numbers

Base	Term 1	Term 2	Term 3	Term 4	Term 5	Term 6	Term 7	Term 8	Term n
Triangle	1	4	10	20	35	56	84	120	$\frac{1}{6}n(n+1)(n+2)$
Square	1	5	14	30	55	91	140	204	$\frac{1}{6}n(n+1)(2n+1)$
Pentagon	1	6	18	40	75	126	196	288	?
Hexagon	1	7	22	50	95	161	252	372	?
Heptagon	1	8	26	60	115	196	308	456	?
Octagon	1	9	30	70	135	231	364	540	?
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k -gon	1	$k+1$	$4k-2$	?	?	?	?	?	$Q(k, n)$

There may not appear to be anything complicated about these numbers derived from geometric configurations. However, they give rise to many interesting and difficult problems. For example, the first two triangular pyramidal numbers, 1 and 4, are both square. Are there any other triangular pyramidal numbers that are square? It turns out that there is just one more:

$$140^2 = 1 + 3 + 6 + 10 + \cdots + 1176.$$

However, the proof that this is the only one is difficult.

The table of polygonal numbers (Table 2.1) reveals two numbers that are both square and triangular, namely 1 and 36. Are there any more? As it happens the next one is 1225, followed by 41 616 and then 1 413 721. Exercise 2.2(b) gives us a clue to one way of attacking this problem. The number x^2 will be triangular as well as square if, and only if, $8x^2 + 1$ is a square. In other words, triangular squares will arise from integer solutions of the equation $8x^2 + 1 = y^2$. If x and y are integers satisfying this equation then x^2 is a triangular square. In fact there are infinitely many solutions of this equation, and hence infinitely many triangular squares. You will see how to find them all later in the module, in Book C, Chapter 12.

Exercise 2.4

(a) In Exercise 2.3(b) we discovered the formula

$$P(k, n) = P(k-1, n) + P(3, n-1).$$

Examination of Table 2.2 shows that the same relationship appears to hold there, namely that each entry in the body of the table is equal to the one above it added to the triangle-based pyramidal number at the top of the previous column. That is,

$$Q(k, n) = Q(k-1, n) + Q(3, n-1).$$

Assuming this formula is true, show that

$$Q(5, n) = \frac{1}{2}n^2(n + 1)$$

and determine $Q(6, n)$.

- (b) If either $2n^2 + 1$ or $2n^2 - 1$ is a square, say m^2 , show that $(nm)^2$ is a triangular number. Hence find three examples of squares that are also triangular.
- (c) Show that no triangular number can have 2, 4, 7 or 9 as its last digit.

Hint: you might find a case-by-case analysis of final digits occurring in numbers of the form $k(k + 1)$ helpful.

3 Mathematical induction

Although you may have encountered mathematical induction before now, you may not be familiar with the more formal approach taken to it in this section.

3.1 Notation

Before progressing further we introduce some standard notation to be used throughout this module. In number theory we are primarily interested in the positive integers, also called the *natural numbers*.

A collection of distinct objects (such as numbers) is known as a **set**. The set of all **integers**, positive, negative or zero, is denoted by $\mathbb{Z}$:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\},$$

and the set of **natural numbers** is denoted by $\mathbb{N}$:

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

We have described each of these sets by (partially) listing its elements within ‘curly brackets’, which are known more formally as **braces**. We often describe a set by giving a property that characterises its elements. For example, the set of all integers that are multiples of 3, and which is denoted by $3\mathbb{Z}$, can be described either by

$$3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

or by

$$3\mathbb{Z} = \{3n : n \in \mathbb{Z}\}.$$

We will also have occasion to refer to the set $\mathbb{Q}$ of **rational numbers** and the set $\mathbb{R}$ of **real numbers**. The rational numbers are the numbers $\frac{a}{b}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, and the real numbers can be thought of as values representing all the points along an infinite number line.

Finally, we will make extensive use of the **modulus** or *absolute value* function, which is defined for any element n of $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$) by

$$|n| = \begin{cases} n, & \text{if } n \geq 0, \\ -n, & \text{if } n < 0. \end{cases}$$

Exercise 3.1

- (a) Which set of numbers is described by each of the following?
 - (i) $\{n \in \mathbb{Z} : |n| > 20\}$
 - (ii) $\{n : n = 2m^2, \text{ for some } m \in \mathbb{N}\}$
- (b) Describe each of the following sets in the notation used in part (a).
 - (i) The set of all odd natural numbers.
 - (ii) The set of all integers lying between -100 and 100 inclusive.

3.2 Mathematical induction

One property of $\mathbb{N}$ that is not shared by some other number sets such as $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$ is worth recording. It may seem a rather obvious property, but its presence is crucial to establishing less apparent properties that we are going to need.

The Well-Ordering Principle for $\mathbb{N}$

Every non-empty subset of $\mathbb{N}$ has a least member. In other words, if S is a non-empty subset of $\mathbb{N}$ then there exists $b \in S$ such that $b \leq n$ for all $n \in S$.

In future we will refer to this just as the Well-Ordering Principle. It says that any collection of natural numbers we care to describe, as long as it has some elements in it, must have a least member. Notice that the set of positive real numbers does not have this property. For example, the set of positive real numbers itself has no least element since, if x is *any* positive real, then

$$0 < \frac{1}{2}x < x,$$

showing that $\frac{1}{2}x$ is a positive real number smaller than x . Hence x cannot be the smallest positive real number.

From the Well-Ordering Principle we can quickly deduce the result that is the backbone of the method of proof by *mathematical induction*.

Theorem 3.1 *Principle of Induction*

If S is a set of natural numbers with the following two properties:

- (a) 1 is a member of S
- (b) if $k \in S$, then the next integer $k + 1 \in S$

then $S = \mathbb{N}$.

Proof We give a proof by contradiction. We assume that the theorem is not true and that there is a set S of natural numbers satisfying (a) and (b) that is not the whole of $\mathbb{N}$. We show that this assumption leads to a contradiction and therefore the theorem must be true.

Let A be the set of all natural numbers that do not belong to S . By the assumption that S is not the whole of $\mathbb{N}$, we know that A is non-empty. Hence, by the Well-Ordering Principle, A must contain a least member. Let this least member of A be a .

By property (a) the integer 1 belongs to S , and so 1 is not in A . Therefore $a > 1$. Now consider the integer $a - 1$, which must be positive as $a > 1$. Furthermore, as $a - 1 < a$ and a is the least member of A , it follows that $a - 1$ does not belong to A . Therefore $a - 1$ is a member of S .

But property (b) now tells us that the integer following $a - 1$, namely a itself, belongs to S . This contradicts the fact that a belongs to A . This contradiction means that the one assumption we made, namely that A is non-empty, must be false. So A is empty and hence S is the set of all natural numbers. ■

Worked Exercise 3.2

Prove that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \quad \text{for all natural numbers } n.$$

Solution

With an eye on the Principle of Induction, let S be the set of natural numbers n for which the formula holds. Our goal is to show that $S = \mathbb{N}$.

Putting $n = 1$ in the formula, we observe that the left-hand side has only one term so that the formula reduces to $1 = 1^2$, which is true. So $1 \in S$.

It remains to prove property (b). To that end, suppose $k \in S$, where k is some natural number. Since $k \in S$ we have that

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2.$$

We discovered this formula in Section 2 but did not give a formal proof. We rectify that omission now.

To deduce that $k + 1 \in S$ we must show that the given formula is true for the case $n = k + 1$. Working on the left-hand side of the formula for $n = k + 1$:

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) \\ &= k^2 + (2k + 1), \quad \text{from the assumption that } k \in S, \\ &= (k + 1)^2, \quad \text{which is the required right-hand side.} \end{aligned}$$

This reasoning shows that if $k \in S$ then $k + 1 \in S$, which confirms property (b).

Hence $S = \mathbb{N}$, and the formula is true for all natural numbers.

We presented Worked Exercise 3.2 by applying the Principle of Induction to the set of natural numbers for which the proposition was true. In future we will present such arguments less formally and will refer to them as proof by **mathematical induction**. The propositions for which we attempt such proofs are ones that are given in terms of a general natural number n , and that we hope to be true for all $n \in \mathbb{N}$.

Let $P(n)$ be a proposition whose truth we wish to prove by mathematical induction. Such a proposition can take various forms. It might be a formula as in Worked Exercise 3.2, an inequality such as $2^n > n^3$, which we will discuss in Worked Exercise 3.4, or a statement such as ‘ n can be written as a sum of distinct powers of 2’, which you will meet in Worked Exercise 3.6. To prove the truth of $P(n)$, let S be the set of natural numbers n for which $P(n)$ is true. If we know that $P(1)$ is true then $1 \in S$. Further, if we can show that whenever $P(k)$ is true it follows that $P(k + 1)$ is true, then $k \in S$ implies $k + 1 \in S$. Hence, by the Principle of Induction, $S = \mathbb{N}$, and $P(n)$ is true for all natural numbers.

We state this formally as follows.

Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on a natural number n . If:

- (a) $P(1)$ is true
 - (b) for any integer $k \geq 1$, if $P(k)$ is true then $P(k + 1)$ is true
- then $P(n)$ is true for all $n \in \mathbb{N}$.

Step (a), showing that the proposition is true for the first value, is called the **basis for the induction**. Step (b) is called the **induction step**. The assumption made in this step, that $P(k)$ is true for some integer k , is called the **induction hypothesis**.

Worked Exercise 3.3

Prove the following formula for the sum of the first n triangular numbers.

$$1 + 3 + 6 + 10 + \cdots + \frac{1}{2}n(n+1) = \frac{1}{6}n(n+1)(n+2) \quad P(n)$$

Solution

We use mathematical induction to prove that $P(n)$ is true for all integers $n \geq 1$ by establishing (a) and (b) above.

First the basis for the induction. Putting $n = 1$ in $P(n)$ gives

$$1 = \frac{1}{6} \times 1(1+1)(1+2).$$

This is correct, showing that $P(1)$ is true.

Now the induction step. We assume that $P(k)$ is true for some natural number k . That is, we have the induction hypothesis

$$1 + 3 + 6 + 10 + \cdots + \frac{1}{2}k(k+1) = \frac{1}{6}k(k+1)(k+2).$$

We need to deduce the truth of $P(k+1)$ from this, that is

$$\begin{aligned} 1 + 3 + 6 + 10 + \cdots + \frac{1}{2}k(k+1) + \frac{1}{2}(k+1)(k+2) \\ = \frac{1}{6}(k+1)(k+2)(k+3). \end{aligned}$$

Taking the left-hand side, we have

$$\begin{aligned} 1 + 3 + 6 + 10 + \cdots + \frac{1}{2}k(k+1) + \frac{1}{2}(k+1)(k+2) \\ = \frac{1}{6}k(k+1)(k+2) + \frac{1}{2}(k+1)(k+2), \\ \text{by the induction hypothesis,} \\ = (k+1)(k+2)\left(\frac{1}{6}k + \frac{1}{2}\right) \\ = \frac{1}{6}(k+1)(k+2)(k+3), \quad \text{which is the RHS of } P(k+1). \end{aligned}$$

This establishes the truth of $P(k+1)$ and completes the induction step.

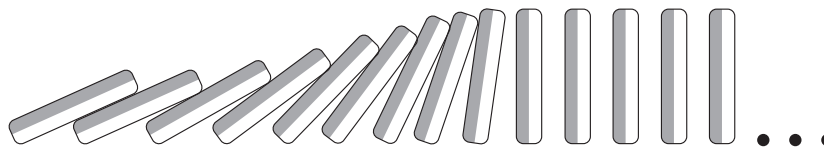
Hence, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers.

By ‘prove’ we mean ‘prove for all integers $n \geq 1$ ’. The ‘for all integers $n \geq 1$ ’ is taken for granted.

The last term on the left-hand side is the $(k+1)$ th triangular number.

RHS is short for right-hand side and LHS is short for left-hand side of an equation.

Mathematical induction can be likened to a line of dominoes (Figure 3.1), arranged so that if any one falls over, it will knock over the next one along the line (the induction step). Then, if the first domino is knocked over (the basis for the induction), they all fall over.



The first domino is knocked over If the k th domino is knocked over,
so too is the $(k + 1)$ th

Figure 3.1 Illustrating mathematical induction

Of course, the induction step is at the heart of any induction proof. Quite often, as in both the preceding worked exercises, some algebraic manipulation is involved. This may be straightforward or quite complex. The next exercise provides you with an opportunity to practise proof by induction.

Exercise 3.2

- (a) Use mathematical induction to prove that the formula

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

is true for all natural numbers.

- (b) A **geometric series** is the sum of a finite sequence of terms in which the ratio of successive terms is constant, r in the following example.

Use mathematical induction to prove the formula for the geometric series

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1}, \quad r \neq 1.$$

3.3 More general induction

The examples that we have seen using mathematical induction have all concerned propositions $P(n)$ that are true for all natural numbers. In this case $n = 1$, the smallest integer for which the proposition was true, provided the basis for the induction. In fact there is nothing special about the number 1 here. The Principle of Induction is readily adapted to provide proofs of results that are true for all integers greater than some integer n_0 .

Principle of Mathematical Induction (generalised)

Let $P(n)$ be a proposition depending on an integer n . If:

- (a) $P(n_0)$ is true
 - (b) for any integer $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ is true
- then $P(n)$ is true for all integers $n \geq n_0$.

As before, step (a) of the generalised principle is called the basis for the induction, and step (b) is called the induction step.

In the next worked exercise we use this generalised form of induction to prove a result that is true for all integers from 10 onwards. In this example the induction step involves more reasoning than the simple algebraic manipulations we have met so far.

Worked Exercise 3.4

For which natural numbers n is it true that $2^n > n^3$?

Solution

Exploration of the relative values of 2^n and n^3 for small values of n shows that 2^n is larger when $n = 1$, but then n^3 is larger for $n = 2, 3, 4, \dots, 9$. For $n = 10$, 2^n becomes the larger value once again:

$$2^{10} = 1024 > 1000 = 10^3.$$

As n now increases it appears that 2^n grows more quickly than n^3 , which leads us to conjecture:

$$2^n > n^3 \text{ for all integers } n \geq 10.$$

Preparing the way for induction, we let $P(n)$ be the statement that $2^n > n^3$.

Having seen that $P(10)$ is true, the basis for the induction is established (as $n_0 = 10$).

It remains to show that, for any integer $k \geq 10$, if $P(k)$ is true then $P(k+1)$ is true. So the induction hypothesis is

$$2^k > k^3, \quad \text{for some } k \geq 10,$$

and from this assumption we need to show that

$$2^{k+1} > (k+1)^3.$$

Now, $2^{k+1} = 2 \times 2^k$ and so the induction hypothesis gives

$$2^{k+1} > 2k^3.$$

Therefore it suffices to show that, for any $k \geq 10$,

$$2k^3 \geq (k+1)^3,$$

or, rearranging,

$$\left(1 + \frac{1}{k}\right)^3 \leq 2.$$

This is certainly true by the following argument. As $k > 1$, the largest value of $\left(1 + \frac{1}{k}\right)^3$ comes from the largest value of $1 + \frac{1}{k}$. This in turn comes from the smallest value of k , namely $k = 10$. However, $\left(1 + \frac{1}{10}\right)^3 = 1.331$, which is less than 2. This completes the induction step.

Hence, by the Generalised Principle of Mathematical Induction, the proposition is true for all integers $n \geq 10$.

Worked Exercise 3.4 has some points of interest. Investigation of the induction step led us to the inequality

$$\left(1 + \frac{1}{k}\right)^3 \leq 2.$$

In fact this inequality holds true for all integers $k \geq 4$ and so the induction step works for all integers $k \geq 4$ (although we were concerned only with integers $k \geq 10$). Drawing on the earlier analogy with dominoes, the situation in Worked Exercise 3.4 is as depicted in Figure 3.2. If any domino from the fourth onwards were to fall it would knock the next over, but the first one of these that *does* fall is the tenth.

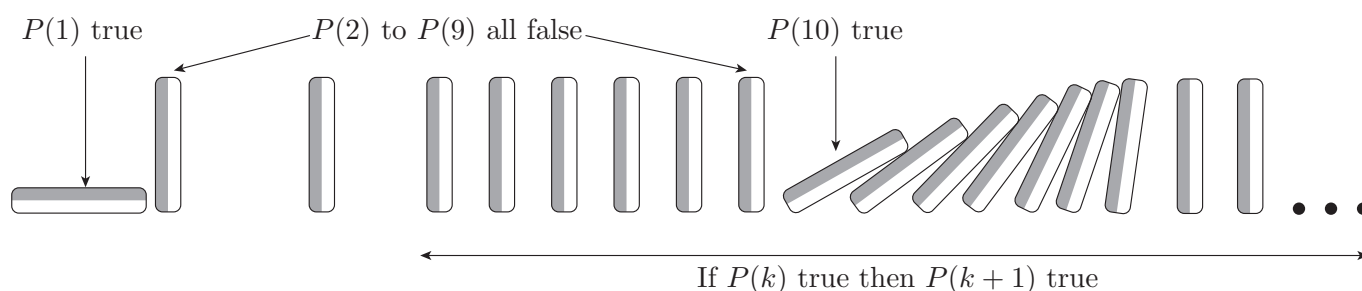


Figure 3.2 $P(n) : 2^n > n^3$ for $n \geq 10$

In the examples so far, when establishing the induction step, we assumed that the proposition under question was true for some integer $k \geq n_0$. On occasion it can be helpful to make a more general assumption. The *Second Principle of Mathematical Induction* employs a different induction step.

Second Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on an integer n . If:

(a) $P(n_0)$ is true

(b') for any integer $k \geq n_0$, if $P(n_0), P(n_0 + 1), \dots, P(k)$ are all true, then $P(k + 1)$ is true

then $P(n)$ is true for all integers $n \geq n_0$.

The Second Principle of Mathematical Induction seems logically sound if one thinks of the domino analogy, and can be established from the Well-Ordering Principle. We will not do so here but proof of this can be found in the solution to Exercise 3.4(d).

The next two worked exercises both make use of the Second Principle of Mathematical Induction.

Worked Exercise 3.5

A sequence of integers is defined as follows:

$$x_0 = 1; \quad x_n = x_0 + x_1 + \cdots + x_{n-1}, \quad \text{for all integers } n \geq 1.$$

Prove that $x_n = 2^{n-1}$, for all integers $n \geq 1$.

Solution

Denote the proposition $x_n = 2^{n-1}$ by $P(n)$.

Then $x_1 = x_0 = 1 = 2^0$, so $P(1)$ is true and we have the basis for the induction.

Heading towards the (new) induction step, suppose that $P(r)$ is true for all $1 \leq r \leq k$; that is,

$$x_r = 2^{r-1}, \quad \text{for } 1 \leq r \leq k.$$

Then

$$\begin{aligned} x_{k+1} &= x_0 + x_1 + \cdots + x_k \\ &= 1 + (1 + 2 + 4 + \cdots + 2^{k-1}), \quad \text{by the induction hypothesis,} \\ &= 1 + \frac{2^k - 1}{2 - 1}, \quad \begin{array}{l} \text{by formula for geometric series,} \\ \text{Exercise 3.2(b),} \end{array} \\ &= 2^k. \end{aligned}$$

This establishes the truth of $P(k + 1)$ and completes the induction step.

Hence the result follows by the Second Principle of Mathematical Induction.

Although there are other ways of proving the result in Worked Exercise 3.5, it is not easy to prove using mathematical induction without making use of the Second Principle. It is the fact that each number in the sequence is defined in terms of *all* the preceding numbers that makes the Second Principle relevant. In Worked Exercise 3.6 we employ the Second Principle of Mathematical Induction again, but this time it will be used differently.

Worked Exercise 3.6

Prove that every natural number n can be written as a sum of distinct (integer) powers of 2. For example, $13 = 2^0 + 2^2 + 2^3$ and $20 = 2^2 + 2^4$.

You might be familiar with the fact that each natural number is expressed *uniquely* in this way: we are essentially representing n in binary. However, we omit the proof of uniqueness here.

Solution

Let $P(n)$ be the proposition that n can be written as a sum of distinct powers of 2.

Then, since $1 = 2^0$, $P(1)$ is true and we have the basis for the induction.

To make use of the Second Principle we assume that, for some natural number k , $P(r)$ is true for each integer r in the range $1 \leq r \leq k$. That is, we assume that each r in this range can be expressed in the required way. To complete the induction proof we show that, under this assumption, $k + 1$ can be expressed as a sum of distinct powers of 2, thereby establishing the truth of $P(k + 1)$.

We consider two cases, depending on whether $k + 1$ is even or odd.

Case $k + 1$ even

Since $k + 1$ is even we can write $k + 1 = 2s$ for some natural number s . Now $s < k + 1$ so, by the induction hypothesis, s can be written as a sum of distinct powers of 2, say

$$s = 2^a + 2^b + \cdots + 2^f, \quad a, b, \dots, f \text{ distinct.}$$

Multiplying this sum by 2 gives

$$k + 1 = 2s = 2^{a+1} + 2^{b+1} + \cdots + 2^{f+1},$$

$$a + 1, b + 1, \dots, f + 1 \text{ distinct,}$$

as required.

Case $k + 1$ odd

Since $k + 1$ is odd we can write $k + 1 = 2s + 1$ for some natural number s . Now $2s < k + 1$ so, by the induction hypothesis, $2s$ can be written as a sum of distinct powers of 2, say

$$2s = 2^a + 2^b + \cdots + 2^f, \quad a, b, \dots, f \text{ distinct.}$$

Since $2s$ is even, and the exponents in this representation of $2s$ are distinct, no exponent can be 0 (because the only power of 2 giving an odd integer is $2^0 = 1$).

Hence

$$\begin{aligned} k + 1 &= 2s + 1 \\ &= 2^a + 2^b + \cdots + 2^f + 1, \quad a, b, \dots, f \text{ distinct and non-zero,} \\ &= 2^a + 2^b + \cdots + 2^f + 2^0, \quad a, b, \dots, f, 0 \text{ distinct,} \end{aligned}$$

as required.

This completes the induction step and the result follows by the Second Principle of Mathematical Induction.

Exercise 3.3

In the sequence

$$1, 3, 4, 7, 11, 18, 29, 47, \dots,$$

each term, from the third onwards, is the sum of the previous two terms. That is, the sequence $\{L_n\}$ is defined by

$$L_1 = 1; \quad L_2 = 3; \quad L_n = L_{n-1} + L_{n-2}, \quad \text{for } n \geq 3.$$

Use the Second Principle of Mathematical Induction to prove that

$$L_n < \left(\frac{7}{4}\right)^n, \quad \text{for all } n \geq 1.$$

Mathematical induction provides a powerful method of proof, whose applications include proving the truth of formulas for all integers from some integer onwards. But while mathematical induction is a great help in proving formulas, it does not help us to find such formulas. Discovering the formulas in the first place is a different matter.

We finish this section with an exercise that sets several problems on proof by mathematical induction.

Exercise 3.4

- (a) Use the Principle of Mathematical Induction to prove that the following formulas are true for all natural numbers n .

$$(i) \quad 1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{1}{3}n(4n^2 - 1)$$

$$(ii) \quad 1 + 5 + 12 + 22 + \cdots + \frac{1}{2}n(3n-1) = \frac{1}{2}n^2(n+1)$$

Note that part (ii) establishes the formula for sums of pentagonal numbers derived as $Q(5, n)$ in Exercise 2.4(a) of Section 2 above.

- (b) The **factorial** of $k \in \mathbb{N}$ is $k! = 1 \times 2 \times \cdots \times k$.

Prove the following formula for all natural numbers n .

$$1 \times (1!) + 2 \times (2!) + 3 \times (3!) + \cdots + n \times (n!) = (n+1)! - 1$$

- (c) For which natural numbers n is it true that $n! > 6n^2$? Prove your result using mathematical induction.
- (d) Show how the Second Principle of Mathematical Induction can be derived from the Well-Ordering Principle, as follows.

Suppose that the conditions (a) and (b') stated in the Second Principle of Mathematical Induction hold. Let S be the set of integers k , $k \geq n_0$, for which $P(k)$ does not hold, that is,

$$S = \{k \in \mathbb{Z} : k \geq n_0 \text{ and } P(k) \text{ is false}\}.$$

Suppose that S is non-empty and use this assumption to deduce that the set

$$T = \{s - n_0 : s \in S\}$$

is a non-empty set of natural numbers. Show how the existence of a least member of T leads to a contradiction.

4 Divisibility

This section introduces some useful properties of division, as well as the connected notions of highest common factor and least common multiple.

4.1 Integer division

From an early age we learn how to divide one natural number by another, obtaining a quotient and a remainder. For example, we can divide 23 by 4 to obtain a quotient of 5 and a remainder of 3 or, rather more formally, $23 = 4 \times 5 + 3$. In fact, if we stipulate that when dividing by 4 the only permitted remainders are 0, 1, 2 and 3 then the quotient and remainder in any division by 4 turn out to be unique. That is, the only way that we can write $23 = 4 \times q + r$, where q and r are integers with $0 \leq r < 4$, is $q = 5$ and $r = 3$. Such uniqueness holds for division by any natural number. The familiar result exemplified here, known as the *Division Algorithm*, is of enormous theoretical importance. In what follows we will discuss certain consequences of it that are fundamental to our treatment of numbers.

Theorem 4.1 The Division Algorithm

For any two integers a and b , where $b > 0$, there exist unique integers q and r such that

$$a = bq + r, \quad \text{where } 0 \leq r < b.$$

Proof Consider the set of integers

$$S = \{a - bn \geq 0 : n \in \mathbb{Z}\}.$$

The set S is non-empty because, as b is positive, $a - bn$ will certainly be positive for large negative values of n . Either 0 is a member of S , and hence the least member of S , or S is a non-empty set of natural numbers and, by the Well-Ordering Principle, again has a least member. So in either case there exists an integer q such that $a - bq = r$ is the least member of S . Hence we have integers q and r such that

$$a = bq + r, \quad \text{where } 0 \leq r.$$

If $r \geq b$ then $r - b \geq 0$. In addition,

$$r - b = a - bq - b = a - b(q + 1)$$

and so $r - b$ is a member of S . However, $r - b$ is smaller than r , which contradicts the minimality of r , and so $r < b$.

It remains to prove the uniqueness of q and r . Suppose, therefore, that

$$a = bq + r, \quad 0 \leq r < b,$$

and

$$a = bq' + r', \quad 0 \leq r' < b.$$

S is the set of non-negative integers in the set $\{\dots, a - 2b, a - b, a, a + b, \dots\}$.

Subtracting gives

$$0 = b(q - q') + (r - r').$$

Now if $q = q'$ this equation gives $r = r'$ and so the expressions for a are the same.

On the other hand, if $q \neq q'$, we may assume that $q > q'$ and hence that $q - q' > 0$. It follows that $q - q' \geq 1$. Since $b > 0$ we have

$$\begin{aligned} r' - r &= b(q - q') \\ &\geq b \times 1 = b. \end{aligned}$$

Adding r to both sides gives

$$r' \geq b + r \geq b,$$

contradicting the definition of r' .

Therefore the values of q and r are unique. ■

Essentially the same argument is illustrated as follows. Imagine multiples of b stepped off along the number line, as shown in Figure 4.1. As the intervals marked off in this way cover the whole line, the number a lies in some interval

$$bq \leq a < b(q + 1).$$

This interval containing a will be unique. Notice that if a is a multiple of b then a coincides with one of the marks between the intervals. In this case, the interval to either side of a could be chosen to contain a . However, the inequalities decree that we choose the interval that has a at its left-hand end.

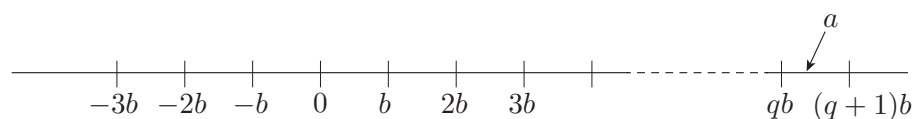


Figure 4.1 Illustrating the Division Algorithm

Subtracting bq through the above inequality shows us that there is a unique integer q such that $0 \leq a - bq < b$. Now putting $a - bq = r$ gives the claimed result.

The way of representing numbers suggested by the Division Algorithm will be important to us, so let us pause to look at some simple applications.

Worked Exercise 4.2

Show that when any square is divided by 4 the remainder is either 0 or 1.

Solution

The Division Algorithm, applied to division by 4, tells us that any integer can be written uniquely in one of the forms $4n$, $4n + 1$, $4n + 2$ or $4n + 3$ for some integer n . So any square number is the square of an integer of one of these four forms. We write each square in its unique form $4q + r$ and hope to find that the only possible values for r are 0 and 1.

$$(4n)^2 = 16n^2 = 4(4n^2) + 0$$

$$(4n + 1)^2 = 16n^2 + 8n + 1 = 4(4n^2 + 2n) + 1$$

$$(4n + 2)^2 = 16n^2 + 16n + 4 = 4(4n^2 + 4n + 1) + 0$$

$$(4n + 3)^2 = 16n^2 + 24n + 9 = 4(4n^2 + 6n + 2) + 1$$

In each case the remainder on division by 4 is either 0 or 1, as claimed.

In fact we could have made the calculations simpler by working with remainders on division by 2. Any number is either of form $2n$ or of form $2n + 1$ and the respective squares are

$$(2n)^2 = 4n^2 + 0,$$

$$(2n + 1)^2 = 4n^2 + 4n + 1 = 4(n^2 + n) + 1,$$

showing that the remainder on division by 4 is either 0 or 1.

Exercise 4.1

The Division Algorithm tells us that any integer can be written in one of the forms $3n$, $3n + 1$ or $3n + 2$. Use this fact to deduce that when any cube is divided by 9 the remainder is one of 0, 1 or 8.

Before moving on, we would like to highlight two formulas with which you are likely to be familiar and which can readily be verified by expanding the brackets.

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Knowledge of these formulas can be useful, as was the case in the solutions to Worked Exercise 4.2 and Exercise 4.1.

The Division Algorithm provides us with our definition of divisibility: one number is divisible by another when the unique remainder is 0.

Definition 4.3 *Factors and multiples*

An integer a is divisible by the natural number b (or, for brevity, b **divides** a) if there exists some integer q such that $a = bq$.

When b divides a we say that b is a **factor** of a or that a is a **multiple** of b .

We write $b \mid a$ as a shorthand for b divides a , and $b \nmid a$ for b does not divide a .

In other texts you may find the phrase ‘ b is a **divisor** of a ’ rather than ‘ b is a factor of a ’.

Be careful not to confuse the statement $b \mid a$ with the fraction $\frac{b}{a}$. For example, $3 \mid 21$ since $21 = 3 \times 7$ and $6 \mid -24$ since $-24 = 6 \times (-4)$. On the other hand, $6 \nmid 16$ since $16 = 6 \times 2 + 4$.

Notice that we consider division only by positive integers. The definition could be adapted to permit division by negative numbers by declaring that a is divisible by b (positive or negative) when there exists an integer q such that $a = bq$. But if $a = bq$ it must be the case that $a = (-b)(-q)$ and so this definition would lead to b being a factor of a if, and only if, $-b$ is a factor of a . There is therefore nothing essentially complicated in dividing by negative numbers, but we will have no occasion to do so. Therefore, if we ask for the factors of an integer, we expect answers that are positive.

Notice also that 0 is excluded as a factor, as the only number for which 0 is a factor is 0 itself. Additionally, since $0 = n \times 0$, every natural number is a factor of 0; in fact 0 is unique in having an infinite number of factors, as will be shown in the proof of Theorem 4.4(b).

Exercise 4.2

- (a) List all the factors of 18 and -24 . Do these two numbers have any factors in common?
- (b) Show that if n is not a multiple of 3 then $n^2 - 1$ is divisible by 3.

Exercise 4.2(a) highlights one property of divisibility, namely that any integer greater than 1 has at least two factors, namely itself and 1. This is just one of a number of simple properties that are direct consequences of the definition. Such properties are not particularly exciting in themselves but some of them will prove to be useful as tools for deriving further information. A selection of the more important properties have been grouped together in the following theorem.

Theorem 4.4 *Properties of division*

Let a and b be natural numbers and c and d be any integers.

- (a) If $a \mid c$ then $a \mid (c + na)$ for any integer n .
- (b) If $c \neq 0$ and $a \mid c$ then $a \leq |c|$.
- (c) If $a \mid b$ and $b \mid a$ then $a = b$.
- (d) If $a \mid b$ and $b \mid c$ then $a \mid c$.
- (e) If $a \mid c$ and $a \mid d$ then $a \mid (mc + nd)$ for any integers m and n .

Proof

- (a) As $a \mid c$ there is an integer q such that $c = aq$. But then

$$c + na = aq + na = a(q + n) = ax,$$

and as $x = q + n$ is an integer, this confirms that a divides $c + na$.

- (b) As $c = aq$ as in (a), $|c| = |aq| = a|q|$, and the result follows since $|q| \geq 1$, q being a non-zero integer.

Notice that this result shows that the non-zero integer c can have only a finite number of factors, since they must all be less than or equal to $|c|$.

- (c) If $a \mid b$ and $b \mid a$ then, from (b), $a \leq b$ and $b \leq a$. The required equality follows.
- (d) If $a \mid b$ and $b \mid c$ then there are integers s and t such that $b = as$ and $c = bt$. Substituting for b gives $c = ast = a(st)$, and as st is an integer this shows that $a \mid c$.
- (e) If $a \mid c$ and $a \mid d$ then there are integers p and q such that $c = ap$ and $d = aq$. But then, for any integers m and n ,

$$mc + nd = map + naq = a(mp + nq) = ax,$$

where $x = mp + nq$ is an integer. So $a \mid (mc + nd)$. ■

4.2 The highest common factor

In Exercise 4.2(a) we saw that the two numbers 18 and -24 had four common factors, namely 1, 2, 3 and 6. It is clear that any two integers will have at least one common factor because 1 divides every integer. What is more, property (b) of the previous theorem guarantees that any integer (other than 0) has only finitely many factors. Therefore any two integers, not both of which are 0, have a non-empty, finite set of common factors. We are going to be interested in the *highest common factor* of two integers, that is, the largest member of the finite set of common factors.

Highest common factors are also known as **greatest common divisors** with the corresponding notation $\gcd(a, b)$.

When we write $\text{hcf}(a, b)$ it will be understood that a and b are integers not both of which are zero.

Definition 4.5 Highest common factor

The **highest common factor** of two integers a and b , not both of which are zero, is the natural number n satisfying the following:

- (a) $n \mid a$ and $n \mid b$
- (b) if $d \mid a$ and $d \mid b$ then $d \leq n$.

The highest common factor of a and b is denoted by $\text{hcf}(a, b)$.

Property (a) of this definition says that $\text{hcf}(a, b)$ is a common factor of a and b , while property (b) says that it is *maximal* amongst the common factors.

Exercise 4.2(a) establishes that $\text{hcf}(18, -24) = 6$. Similarly, as you may wish to verify, $\text{hcf}(3, 20) = 1$ and $\text{hcf}(14, 35) = 7$.

Two properties that follow immediately from the definition are worth recording.

Since zero is divisible by every natural number, it follows that

$$\text{hcf}(0, b) = |b|.$$

Since n and $-n$ have the same set of positive factors,

$$\text{hcf}(a, b) = \text{hcf}(-a, b) = \text{hcf}(a, -b) = \text{hcf}(-a, -b).$$

Property (e) of Theorem 4.4 shows that any common factor of two integers c and d also divides any integer of the form $mc + nd$. Numbers of this latter form merit their own name.

Definition 4.6 Integer combination

If a and b are integers, then any integer of the form

$$ma + nb, \quad m, n \in \mathbb{Z},$$

is called an **integer combination** of a and b .

So $\text{hcf}(a, b)$ divides every integer combination of a and b . In fact more is true: one of these integer combinations is $\text{hcf}(a, b)$.

To illustrate that claim, take the three examples of highest common factor mentioned above.

$$\text{hcf}(18, -24) = 6 = 3 \times 18 + 2 \times (-24)$$

$$\text{hcf}(3, 20) = 1 = 7 \times 3 + (-1) \times 20$$

$$\text{hcf}(14, 35) = 7 = (-2) \times 14 + 1 \times 35$$

Proposition 4.7

Given any integers a and b , not both zero, there exist integers m and n such that

$$\text{hcf}(a, b) = ma + nb.$$

In other words, $\text{hcf}(a, b)$ is an integer combination of a and b .

Proof Consider the set

$$S = \{xa + yb > 0 : x, y \text{ integers}\}$$

of all positive integer combinations of a and b . Each member of S is an integer and S is non-empty because a , $-a$, b and $-b$ are all integer combinations of a and b of which at least one is positive. Hence the Well-Ordering Principle guarantees the existence of a smallest element d in S . As d is a member of S we know that $d = ma + nb$ for some integers m and n . It is our contention that $d = \text{hcf}(a, b)$.

We first show that d is a common factor of a and b . The Division Algorithm tells us that, from division of a by d , we have $a = dq + r$ for some integers q and r with $0 \leq r < d$. But then

$$\begin{aligned} r &= a - dq \\ &= a - (ma + nb)q \\ &= (1 - mq)a + (-nq)b, \end{aligned}$$

showing that r is an integer combination of a and b . Now if it were the case that $r > 0$ then r would be a member of S and the condition $r < d$ would contradict d being the least member of S . Hence $r = 0$ and d is a factor of a . Similarly d is also a factor of b .

It remains to show that d is the *greatest* of the common factors. Suppose then that d' is any common factor of a and b . Then, by property (e) of Theorem 4.4, d' is a factor of the integer combination $ma + nb$; that is, d' is a factor of d . Property (b) of Theorem 4.4 then gives $d' \leq d$, as required. ■

The ability to write the highest common factor of two integers as an integer combination of them will prove to be very useful. Unfortunately, though our result guarantees that an integer combination exists, it gives us no clue as to how to find that integer combination. We will return to that problem shortly, but first we establish a number of useful consequences of the proposition. The first two concern pairs of integers for which the highest common factor is 1. We have a term to describe such pairs.

Definition 4.8 *Coprime*

Two integers a and b , not both zero, are said to be **coprime**, or **relatively prime**, whenever $\text{hcf}(a, b) = 1$.

For example, 10 and 21 are coprime, since 10 and 21 do not have any common factors other than 1.

We exclude the case where a and b are both zero because $\text{hcf}(0, 0)$ does not exist. For any non-zero integer a , $\text{hcf}(0, a) = |a|$ and hence the only integers that are coprime to 0 are 1 and -1 .

Lemma 4.9

Integers a and b are coprime if, and only if, there exist integers m and n such that $1 = ma + nb$.

Proof If a and b are coprime then $\text{hcf}(a, b) = 1$ and Proposition 4.7 confirms the existence of integers m and n with $ma + nb = 1$.

Conversely, suppose there are integers m and n with $ma + nb = 1$, and let d be any common factor of a and b . Then property (e) of Theorem 4.4 tells us that d divides $ma + nb$; that is, d divides 1. Finally property (b) of Theorem 4.4 gives $d = 1$, and $\text{hcf}(a, b) = 1$, as claimed. ■

We will see in Exercise 4.3(b) that the integers m and n in the statement of Lemma 4.9 are also coprime. Indeed, if there exist non-zero integers a , b , m and n such that $ma + nb = 1$ then each of a and m is coprime to each of b and n .

Proposition 4.10

For any integers a and b , not both zero, if $\text{hcf}(a, b) = d$ then $\frac{a}{d}$ and $\frac{b}{d}$ are integers such that $\text{hcf}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

That is, the integers $\frac{a}{\text{hcf}(a, b)}$ and $\frac{b}{\text{hcf}(a, b)}$ are coprime.

Proof Since d divides a and d divides b there exist integers s and t such that $a = ds$ and $b = dt$. Moreover, Proposition 4.7 gives the existence of integers m and n such that $d = ma + nb$. Dividing this equation through by d leaves us with $1 = ms + nt$, whereupon Lemma 4.9 informs us that $\text{hcf}(s, t) = 1$. That is,

$$\text{hcf}\left(\frac{a}{d}, \frac{b}{d}\right) = 1. \quad \blacksquare$$

In the statement of the proposition we used $\frac{a}{d}$ and $\frac{b}{d}$, knowing that they were integers. In general it is advisable to avoid the use of fractions when trying to prove results concerning integers, since it is important to maintain distinction between the two. Note how, in the proof, we introduced the integers s and t instead of using $\frac{a}{d}$ and $\frac{b}{d}$ respectively.

We often use this in the following form.

If $\text{hcf}(a, b) = d$ there exist integers s and t such that $a = ds$ and $b = dt$, with $\text{hcf}(s, t) = 1$.

The s and t are respectively $\frac{a}{d}$ and $\frac{b}{d}$.

We take a break from the string of results at this point and let you try your hand at some simple proofs. Each of the problems in Exercise 4.3 involves little more than an appropriate application of one of the preceding results.

Exercise 4.3

Let a and b be integers, not both of which are zero. Prove the following.

- (a) The integer c is a multiple of $\text{hcf}(a, b)$ if, and only if, there exist integers x and y such that $c = xa + yb$.
- (b) If $\text{hcf}(a, b) = ma + nb$ then $\text{hcf}(m, n) = 1$.
- (c) If $\text{hcf}(a, b) = 1$ and $\text{hcf}(a, c) = 1$ then $\text{hcf}(a, bc) = 1$.
- (d) For any natural number k , $\text{hcf}(ka, kb) = k \times \text{hcf}(a, b)$.

Note that the result in part (a) asserts that the set of all integer combinations of a and b is precisely the set of all integer multiples of $\text{hcf}(a, b)$.

The next two results establish further divisibility properties.

Lemma 4.11

If $a \mid c$ and $b \mid c$, with $\text{hcf}(a, b) = 1$, then $ab \mid c$.

Proof As a divides c and b divides c , there are integers r and s such that

$$c = ar \quad \text{and} \quad c = bs.$$

Also, $\text{hcf}(a, b) = 1$ implies the existence of integers m and n such that

$$ma + nb = 1.$$

Multiplying through this equation by c , we obtain

$$cma + cnb = c.$$

Substituting bs for the first c and ar for the second c in the left-hand side of this equation gives $ab(sm + rn) = c$, which confirms that ab divides c . ■

Theorem 4.12 Euclid's Lemma

If $a \mid bc$, with $\text{hcf}(a, b) = 1$, then $a \mid c$.

Proof Since a divides bc and $\text{hcf}(a, b) = 1$, we have integers k , m and n such that

$$bc = ka \quad \text{and} \quad ma + nb = 1.$$

Multiplying through the latter by c gives

$$mac + nbc = c$$

and then substitution for bc leaves us with

$$mac + nka = c.$$

That is, $a(mc + nk) = c$, which confirms that a divides c , as required. ■

The following worked exercise incorporates several of the preceding ideas.

Worked Exercise 4.13

- (a) Suppose that a divides bc , where $\text{hcf}(b, c) = 1$. Show that a can be written as a product rs , where r divides b and s divides c .
- (b) Show that if a is an integer with $\text{hcf}(6, a) = 1$ then 24 divides $a^2 - 1$.

Solution

- (a) To illustrate the result, notice that 21 divides 6×35 , and $21 = 3 \times 7$, where 3 divides 6 and 7 divides 35, and this is the only way of expressing 21 as a product of two numbers to fit the statement.

Let $r = \text{hcf}(a, b)$. By Proposition 4.10, there exist integers s and t such that

$$a = rs \quad \text{and} \quad b = rt, \quad \text{where } \text{hcf}(s, t) = 1.$$

Hence we have written $a = rs$, where r divides b . It remains to show that s divides c .

Since a divides bc there exists an integer k such that

$$bc = ka.$$

That is, substituting for a and b ,

$$rtc = krs.$$

Cancelling the r on both sides gives

$$tc = ks,$$

which implies that s divides tc . However, s and t are coprime and so, by Euclid's Lemma, s divides c , as required.

- (b) We show that 3 divides $a^2 - 1$ and 8 divides $a^2 - 1$. The result then follows from Lemma 4.11, since $\text{hcf}(3, 8) = 1$.

Thinking about division by 3, we note that a must be of one of the forms $3n$, $3n + 1$ or $3n + 2$. However, since $\text{hcf}(6, 3n) \geq 3$, the condition that $\text{hcf}(6, a) = 1$ rules out the first of these possibilities. For the case $a = 3n + 1$ we have

$$a^2 - 1 = (3n + 1)^2 - 1 = 9n^2 + 6n + 1 - 1 = 3(3n^2 + 2n),$$

In fact the only integers r and s to fit the statement are $r = \text{hcf}(a, b)$ and, by symmetry, $s = \text{hcf}(a, c)$.

and for the case $a = 3n + 2$ we have

$$a^2 - 1 = (3n + 2)^2 - 1 = 9n^2 + 12n + 4 - 1 = 3(3n^2 + 4n + 1).$$

So in each case $a^2 - 1$ is divisible by 3.

Turning to division by 8, there are eight possible forms for a , namely $8n + r$, for $r = 0, 1, \dots, 7$. However, we notice that $\text{hcf}(a, 6) = 1$ tells us that a cannot be even. Thus we are left with the odd cases, which are $8n + 1$, $8n + 3$, $8n + 5$ and $8n + 7$. Taking these four cases in turn, we have

$$(8n + 1)^2 - 1 = 64n^2 + 16n + 1 - 1 = 8(8n^2 + 2n),$$

$$(8n + 3)^2 - 1 = 64n^2 + 48n + 9 - 1 = 8(8n^2 + 6n + 1),$$

$$(8n + 5)^2 - 1 = 64n^2 + 80n + 25 - 1 = 8(8n^2 + 10n + 3),$$

$$(8n + 7)^2 - 1 = 64n^2 + 112n + 49 - 1 = 8(8n^2 + 14n + 6).$$

In each case $a^2 - 1$ is divisible by 8.

This completes the proof.

Next an exercise for you to try, which should give you practice at applying some of the preceding results.

Exercise 4.4

(a) Suppose that $\text{hcf}(a, b) = 1$. Use Lemma 4.9 to prove the following.

(i) If $c \mid a$ then $\text{hcf}(b, c) = 1$.

(ii) $\text{hcf}(a, a + b) = 1$.

(b) Prove that the following statements are true for any integer n .

(i) $\text{hcf}(3n + 2, 5n + 3) = 1$.

Hint: use property (e) of Theorem 4.4 in the following way.

Suppose that d is any common factor of $3n + 2$ and $5n + 3$. Then d divides $(r(3n + 2) + s(5n + 3))$ for any integers r and s . Try to choose r and s so that d divides 1.

(ii) $\text{hcf}(n^2 + 3n + 1, 2n + 1) = 1$.

Hint: this time you may have to apply property (e) of Theorem 4.4 more than once.

4.3 The least common multiple

In contrast to common factors we also have the notion of common multiples. For example, since $6 \mid 60$ and $10 \mid 60$ we say that 60 is a common multiple of 6 and 10. Of course there are infinitely many common multiples of 6 and 10, the positive ones including 30, 60, 90, 120, 150, 180, and so on. Indeed, it would appear that the common multiples of 6 and 10 are precisely the multiples of 30, 30 being the *least common multiple* of 6 and 10.

Definition 4.14 Least common multiple

The **least common multiple** of the non-zero integers a and b is the natural number n satisfying the following:

- (a) $a \mid n$ and $b \mid n$
- (b) if $a \mid m$ and $b \mid m$ then $n \leq |m|$.

The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

Property (a) of this definition says that $\text{lcm}(a, b)$ is a common multiple of a and b , while property (b) says that it is the smallest natural number with this property. The fact that $|ab|$ is a common multiple of a and b , coupled with the Well-Ordering Principle, ensures that $\text{lcm}(a, b)$ exists.

The example preceding the definition suggested something stronger than property (b), namely that $\text{lcm}(a, b)$ divides any common multiple of a and b . As a first exercise in handling common multiples, we invite you to prove that this property does indeed follow from the definition.

Exercise 4.5

Show that if m is a common multiple of the non-zero integers a and b then $\text{lcm}(a, b)$ divides m .

Hint: use the Division Algorithm and show that the remainder must be zero.

Not surprisingly, the twin concepts of highest common factor and least common multiple are interrelated. Recall from the earlier numerical example that $\text{lcm}(6, 10) = 30$ and $\text{hcf}(6, 10) = 2$. It is no accident that $\text{lcm}(6, 10) \times \text{hcf}(6, 10) = 6 \times 10$.

Proposition 4.15

For any pair of natural numbers a and b ,

$$\text{lcm}(a, b) \times \text{hcf}(a, b) = ab.$$

The corresponding result in which either a or b is negative is $\text{lcm}(a, b) \times \text{hcf}(a, b) = |ab|$. It is readily deduced from this one.

Proof Let $d = \text{hcf}(a, b)$. Then since d divides a , it also divides ab . So there exists a natural number n such that

$$ab = dn.$$

Our task is to show that $n = \text{lcm}(a, b)$.

Since d divides both a and b , there exist integers u and v such that

$$a = du \quad \text{and} \quad b = dv.$$

Substituting for a and then b in $ab = dn$, and cancelling d in each case, gives

$$n = bu \quad \text{and} \quad n = av.$$

This shows that n is a common multiple of a and b , which leaves us to show it is the least such multiple.

Let m be any other common multiple of a and b . There exist integers r and s such that

$$m = ar \quad \text{and} \quad m = bs.$$

We also know that $d = \text{hcf}(a, b)$ is an integer combination of a and b , say

$$d = ax + by.$$

Multiplying this equation by m , and substituting first bs and then ar for m on the right-hand side, we get the following.

$$\begin{aligned} md &= max + mby \\ &= bsax + arby \\ &= ab(sx + ry) \\ &= dn(sx + ry), \quad \text{from the third line of the proof.} \end{aligned}$$

Lastly, cancellation of the d gives

$$m = n(sx + ry).$$

This shows that n is a factor of m and so $n \leq |m|$ as required. ■

Exercise 4.6

Use Proposition 4.15 to determine

- (a) $\text{lcm}(18, 24)$; (b) $\text{lcm}(27, 45)$; (c) $\text{lcm}(39, 40)$.

The following exercise revises the concepts of divisibility and mathematical induction.

Exercise 4.7

- (a) Show that an integer of the form $12k + 8$ is necessarily of the form $3m + 2$, but not conversely.

For which values of r in the range $0 \leq r \leq 11$ is $12k + r$ also of the form $3m + 2$?

- (b) The number 64 is both a square and a cube:

$$64 = 8^2 = 4^3.$$

Show that any number that is both a square and a cube must be of one of the forms $7k$ or $7k + 1$.

- (c) Use mathematical induction to prove that 9 divides $4^n + 6n - 1$ for all integers $n \geq 0$.
- (d) Note that

$$36 \mid 108, \quad 36 \mid 1008, \quad 36 \mid 10\,008, \quad 36 \mid 100\,008, \quad \dots$$

Formulate the general result illustrated by this and prove your result using mathematical induction.

- (e) Prove that if $\text{hcf}(a, b) = 1$ then, for any integer c ,

$$\text{hcf}(ac, b) = \text{hcf}(c, b).$$

- (f) Suppose that $\text{hcf}(a, b) = 1$. Show that:

- (i) $\text{hcf}(2a + b, a + b) = 1$
 (ii) $\text{hcf}(a + b, a - b) = 1$ or 2 .

5 Linear Diophantine equations

Pythagoras and Euclid developed much of the material discussed in this section. You may wish to learn more about these two mathematicians in the *History Reader* for this topic.

5.1 The Euclidean Algorithm

We have seen that the problem of finding least common multiples can readily be solved by first finding the corresponding highest common factor. However, as yet we have no systematic method of finding highest common factors. Given two positive numbers, a and b , we could determine a list of all factors for each and select the largest one in common. That is fine for reasonably small integers, but would you want to tackle finding $\text{hcf}(3108, 5291)$ by such an approach? There is a more efficient method that uses nothing more than repeated division, as in the Division Algorithm; it is called the *Euclidean Algorithm*. First we ask you to study a numerical example illustrating the procedure before returning to see why it works.

Worked Exercise 5.1

Determine $\text{hcf}(3108, 5291)$.

Solution

We begin by dividing the larger number by the smaller.

$$5291 = 1 \times 3108 + 2183$$

Next we divide 3108 by the remainder in the above equation.

$$3108 = 1 \times 2183 + 925$$

We continue in this fashion, at each stage dividing the previous factor by the resulting remainder.

$$2183 = 2 \times 925 + 333$$

$$925 = 2 \times 333 + 259$$

$$333 = 1 \times 259 + 74$$

$$259 = 3 \times 74 + 37$$

$$74 = 2 \times 37 + 0$$

The process stops when a remainder of 0 is encountered and the last non-zero remainder, namely 37, is the required $\text{hcf}(3108, 5291)$.

Let us spell out generally the system of equations that arise in applying the **Euclidean Algorithm** to determine $\text{hcf}(a, b)$. Notice that since $\text{hcf}(-a, b) = \text{hcf}(a, b)$ we can safely assume that the numbers in question are both positive. Repeated application of the Division Algorithm gives the following.

$$\begin{aligned} a &= q_1 \times b + r_1 & 0 < r_1 < b \\ b &= q_2 \times r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_3 \times r_2 + r_3 & 0 < r_3 < r_2 \\ r_2 &= q_4 \times r_3 + r_4 & 0 < r_4 < r_3 \\ &\dots \\ r_{n-2} &= q_n \times r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} \times r_n + 0 \end{aligned}$$

The first fact to observe is that b and the remainders form a strictly decreasing sequence of natural numbers:

$$b > r_1 > r_2 > \cdots > r_{n-2} > r_{n-1} > r_n > 0.$$

This establishes that the algorithm must terminate; a zero remainder must be reached in a finite number of steps.

The outstanding claim to be justified is that the final non-zero remainder, namely r_n , is equal to the highest common factor of the two original numbers, a and b . This is an immediate consequence of the following simple property of highest common factors.

$$\text{If } a = qb + r, \text{ then } \text{hcf}(a, b) = \text{hcf}(b, r).$$

Why is this? As $\text{hcf}(a, b)$ divides both a and b , it also divides $a - qb$. That is, $\text{hcf}(a, b)$ divides r and, being a common factor of b and r ,

$$\text{hcf}(a, b) \leq \text{hcf}(b, r).$$

But the argument works conversely as well: $\text{hcf}(b, r)$ divides both b and $qb + r$ and so is a common factor of a and b . Hence

$$\text{hcf}(b, r) \leq \text{hcf}(a, b).$$

From the two inequalities, it follows that

$$\text{hcf}(b, r) = \text{hcf}(a, b).$$

If we apply this fact to the equations in the Euclidean Algorithm system, we get

$$\text{hcf}(a, b) = \text{hcf}(b, r_1) = \text{hcf}(r_1, r_2) = \cdots = \text{hcf}(r_{n-1}, r_n) = \text{hcf}(r_n, 0).$$

Therefore,

$$\text{hcf}(a, b) = \text{hcf}(r_n, 0) = r_n.$$

The system of equations that arises in the Euclidean Algorithm does more for us than just lead to the highest common factor of numbers a and b .

Proposition 4.7 tells us that $\text{hcf}(a, b)$ can be expressed as an integer combination of a and b , and we are at last in a position to see how to find this expression.

Worked Exercise 5.2

Find integers m and n such that

$$\text{hcf}(3108, 5291) = m \times 3108 + n \times 5291.$$

Solution

Consider the system of equations in Worked Exercise 5.1 that led to $\text{hcf}(3108, 5291) = 37$. We take these equations in reverse order, starting at the penultimate one, which gives the following expression for 37.

$$37 = 259 - 3 \times 74$$

The third-to-last equation gives an expression for the previous remainder, $74 = 333 - 259$, which when substituted into our expression for 37 gives the following.

$$37 = 259 - 3 \times (333 - 259) = -3 \times 333 + 4 \times 259$$

We continue to step back through the system of equations, at each stage substituting for the remainder in the developing expression for 37.

$$\begin{aligned} 37 &= -3 \times 333 + 4 \times (925 - 2 \times 333) \\ &= 4 \times 925 - 11 \times 333 \\ &= 4 \times 925 - 11 \times (2183 - 2 \times 925) \\ &= -11 \times 2183 + 26 \times 925 \\ &= -11 \times 2183 + 26 \times (3108 - 2183) \\ &= 26 \times 3108 - 37 \times 2183 \\ &= 26 \times 3108 - 37 \times (5291 - 3108) \\ &= -37 \times 5291 + 63 \times 3108 \end{aligned}$$

Hence we have

$$37 = 63 \times 3108 + (-37) \times 5291,$$

and so $m = 63$ and $n = -37$ are suitable values.

It must be remarked that this is not the only solution. For example, by adding and subtracting 3108×5291 we get

$$\begin{aligned} 37 &= 63 \times 3108 + (-37) \times 5291 + 3108 \times 5291 - 3108 \times 5291 \\ &= 5354 \times 3108 + (-3145) \times 5291, \end{aligned}$$

giving $m = 5354$ and $n = -3145$ as another of infinitely many possibilities.

For ease of working with the original equations we will always write the integer combination at each stage with the larger number first.

Exercise 5.1

Use the Euclidean Algorithm to determine $\text{hcf}(1092, 777)$ and hence find integers m and n such that

$$\text{hcf}(1092, 777) = 1092m + 777n.$$

5.2 Linear Diophantine equations

Consider the following problem:

I spent exactly £30 buying some 50p stamps and some 60p stamps so that the difference in number between the two kinds of stamp is as small as possible. How many stamps did I buy?

Translating the information in this problem into an equation to be solved presents little difficulty. Suppose that I bought x stamps at 50p and y stamps at 60p. Then, in all, I would have spent $50x + 60y$ pence and so

$$50x + 60y = 3000.$$

This is a linear equation in two variables and the problem is asking us to find one particular solution of it. Now in principle, for any value of x , we can solve the equation for a corresponding value of y . However, there is a major constraint in our problem: we are interested only in solutions of this equation in which the x and y values are non-negative integers, that is, for which $x \geq 0$ and $y \geq 0$. We are not going to be buying either parts of stamps or negative numbers of stamps! It is certainly not the case that for each non-negative integer x there is a corresponding non-negative integer y solving the equation, so there is more to this problem than elementary algebra.

The term **Diophantine equation** is reserved for algebraic equations for which we seek integer solutions. The Diophantine equation arising from the posed problem is one of the form $ax + by = c$ where a , b and c are integers, a and b not both zero. This latter equation is the general **linear Diophantine equation**. In Worked Exercise 5.2 and Exercise 5.1 we have witnessed some instances of the linear Diophantine equation and made use of the Euclidean Algorithm in solving them. We now build on the techniques of those examples to discover how to solve linear Diophantine equations in general.

The posed problem involves slightly more than a linear Diophantine equation since it requests solutions that are non-negative.

We will return to the posed question at the end of this section, but let us start with a linear Diophantine equation involving smaller coefficients. Consider the equation $6x + 15y = 4$. Allowing x and y to take all possible values, we see that the left-hand side of this equation takes all integer combinations of 6 and 15, which we know to be the set of all multiples of $\text{hcf}(6, 15)$. So the left-hand side takes values in the set

$$\{\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}.$$

As 4 does not belong to this set, the Diophantine equation $6x + 15y = 4$ has no solutions. On the other hand, the Diophantine equation $6x + 15y = 9$ does have solutions, because 9 is in the set. But notice that this latter equation can be simplified by cancelling the common factor 3 through the equation to obtain $2x + 5y = 3$. Looked at in this simpler form, $\text{hcf}(2, 5) = 1$ and so the values taken by the left-hand side are all the multiples of 1, which certainly includes 3.

Consider now the general linear Diophantine equation $ax + by = c$. As x and y range through all integers, the values taken by the left-hand side are all the multiples of $\text{hcf}(a, b)$. So a necessary and sufficient condition for the equation to have solutions is that $\text{hcf}(a, b)$ is a factor of c .

Suppose that this condition holds. Then each of a , b and c is divisible by $\text{hcf}(a, b)$ and so, if $\text{hcf}(a, b) > 1$, we divide each coefficient by $d = \text{hcf}(a, b)$ to get the ‘same’ linear Diophantine equation

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d},$$

where

$$\text{hcf}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Hence, under the assumption that the linear Diophantine equation is in its lowest terms (with any common factor of a , b and c already having been cancelled out), the equation $ax + by = c$ has solutions if, and only if, $\text{hcf}(a, b) = 1$.

Let us look at an example.

By ‘same’ linear Diophantine equation, we mean that the two equations have the same set of solutions.

Worked Exercise 5.3

Solve the linear Diophantine equation

$$66x + 40y = 6.$$

Solution

As $\text{hcf}(66, 40) = 2$, and 2 divides 6, we first cancel this common factor to get the ‘same’ equation

$$33x + 20y = 3.$$

As $\text{hcf}(33, 20) = 1$ this Diophantine equation is known to have solutions.

We apply the Euclidean Algorithm to the pair of coefficients 33 and 20.

$$33 = 1 \times 20 + 13$$

$$20 = 1 \times 13 + 7$$

$$13 = 1 \times 7 + 6$$

$$7 = 1 \times 6 + 1$$

$$6 = 6 \times 1 + 0$$

This confirms that $\text{hcf}(33, 20) = 1$.

Reversing the equations, we obtain the following.

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (13 - 7) \\ &= -1 \times 13 + 2 \times 7 \\ &= -1 \times 13 + 2 \times (20 - 13) \\ &= 2 \times 20 - 3 \times 13 \\ &= 2 \times 20 - 3 \times (33 - 20) \\ &= -3 \times 33 + 5 \times 20 \end{aligned}$$

This expresses 1 as an integer combination of 33 and 20, but our present task is to express 3 in this way. Multiplying through by 3, we get

$$3 = -9 \times 33 + 15 \times 20,$$

so that $x = -9$, $y = 15$ is one solution of $33x + 20y = 3$ (and therefore of $66x + 40y = 6$).

Now, what other solutions are there?

Suppose that $x = -9 + s$, $y = 15 - t$ is another solution, for some integers s and t . For this alternative solution, we could equally well have taken $y = 15 + t$, which might seem more obvious. However, this expression is chosen to conform with the usual general solution given below.

Substituting $x = -9 + s$ and $y = 15 - t$ into the equation gives

$$33(-9 + s) + 20(15 - t) = 3,$$

which simplifies to

$$33s = 20t.$$

This equation carries the implication that 20 divides $33s$, and, as $\text{hcf}(20, 33) = 1$, Euclid's Lemma gives that 20 divides s . So we can put $s = 20k$, for some integer k , and then from

$$33 \times 20k = 20t$$

we deduce that $t = 33k$.

This argument has shown that any solution must take the form

$$x = -9 + 20k, \quad y = 15 - 33k, \quad \text{for some integer } k,$$

and, moreover, substituting back into the original equation confirms that, for any integer k , this is indeed a solution. So the general solution of this linear Diophantine equation is

$$x = -9 + 20k, \quad y = 15 - 33k, \quad k \in \mathbb{Z}.$$

We have illustrated the following.

Theorem 5.4 *Solution of linear Diophantine equations*

The linear Diophantine equation $ax + by = c$ has solutions if, and only if, $\text{hcf}(a, b)$ divides c .

If this condition holds with $\text{hcf}(a, b) > 1$ then division by $\text{hcf}(a, b)$ simplifies the equation to $a'x + b'y = c'$, where $\text{hcf}(a', b') = 1$.

If x_0, y_0 is one solution of this equation then the general solution is

$$x = x_0 + b'k, \quad y = y_0 - a'k, \quad k \in \mathbb{Z}.$$

The equation is trivial when either a or b is zero, so we assume that both a and b are non-zero.

Proof The first assertion in the theorem is equivalent to Exercise 4.3(a). Simplification of a linear Diophantine equation was discussed towards the start of this subsection. So the only assertion that has not already been verified is that concerning the general solution. To that end, suppose that x', y' is any solution of the equation. Then we have

$$a'x_0 + b'y_0 = c' \quad \text{and} \quad a'x' + b'y' = c',$$

and on substituting for c' and rearranging,

$$a'(x' - x_0) = b'(y_0 - y').$$

This equation shows that a' divides $b'(y_0 - y')$ and, since $\text{hcf}(a', b') = 1$, Euclid's Lemma gives that a' divides $(y_0 - y')$. That is, $y_0 - y' = a'k$ for some integer k . Substitution of this into the above equation then gives $x' - x_0 = b'k$, and so

$$x' = x_0 + b'k, \quad y' = y_0 - a'k, \quad \text{for some integer } k,$$

as claimed.

Finally, a simple substitution shows that integers

$$x_0 + b'k \quad \text{and} \quad y_0 - a'k$$

constitute a solution of $a'x + b'y = c'$ for any integer k . ■

The two parts of the following exercise require you to find the general solution of a linear Diophantine equation but each then asks you to find, within the general solution, one particular solution.

Exercise 5.2

- (a) Find the general solution of the linear Diophantine equation

$$45x - 14y = 7$$

and also the particular solution in which x takes its least positive value.

Hint: solve the equation for x and $-y$ in the usual way.

This is the question posed at the beginning of this section.

- (b) I spent exactly £30 buying some 50p stamps and some 60p stamps so that the difference in number between the two kinds of stamps is as small as possible. How many stamps did I buy?

As the topic progresses you will discover that linear Diophantine equations crop up frequently, in many guises, often as subsidiary tasks in some deeper problem. When we next meet a linear Diophantine equation we will develop some improved techniques for solving them, removing the need to fall back on the Euclidean Algorithm.

Exercise 5.3

- (a) Use the Euclidean Algorithm to find integers x and y satisfying

$$\text{hcf}(17, 143) = 17x + 143y.$$

Give the general solution of this equation and the particular solution in which x takes its least positive value.

- (b) Find all solutions in natural numbers of the Diophantine equation

$$158x - 57y = 7.$$

- (c) Find all solutions in integers of the Diophantine equation

$$39x + 27y = 3.$$

- (d) Using only 2p, 10p and 50p coins, in how many ways can exactly 100 coins be used to total £6?

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should:

- (a) Understand arithmetic progressions arising from polygonal and pyramidal numbers, and be able to find the sums of finite such sequences.
- (b) Be able to use, and understand the theoretical underpinnings of, mathematical induction.
- (c) Understand and be able to apply the Generalised Principle of Mathematical Induction and the Second Principle of Mathematical Induction.
- (d) Recognise the importance of the Division Algorithm, and be able to apply it in a variety of scenarios.
- (e) Know the meaning of and be able to use the terms ‘factor’, ‘highest common factor’, ‘integer combination’ and ‘coprime’; understand elementary results relating these terms.
- (f) Understand the term ‘least common multiple’, and be able to relate it to highest common factor.
- (g) Know how to apply the Euclidean Algorithm to find the highest common factor of two integers a and b , and express it as an integer combination of a and b .
- (h) Understand the general meaning of the term ‘Diophantine equation’.
- (i) Recognise when a linear Diophantine equation has solutions, and when it does not.
- (j) Be able to find particular and general solutions of given linear Diophantine equations through the application of the Euclidean Algorithm.

Solutions to exercises

Solution to Exercise 2.1

- (a) The first term is $a = 3$ and the common difference is $d = 7$. As the last term is $143 = 3 + (20 \times 7)$, we see that the number of terms is $n = 21$. So the formula for an arithmetic series gives the sum as

$$\frac{1}{2} \times 21(6 + (20 \times 7)) = 1533.$$

- (b) There are 26 terms averaging $100 + \frac{1}{2} \times 25 \times (-2) = 75$ and so the sum is $26 \times 75 = 1950$.

Solution to Exercise 2.2

- (a) If k is the triangular number T_n , then $k = \frac{1}{2}n(n+1)$. Therefore

$$\begin{aligned} 9k + 1 &= \frac{1}{2} \times 9n(n+1) + 1 \\ &= \frac{1}{2}(9n^2 + 9n + 2) \\ &= \frac{1}{2}(3n+1)(3n+2) \\ &= \frac{1}{2}r(r+1), \quad \text{where } r = 3n+1, \end{aligned}$$

which is the triangular number T_r .

- (b) First we show that if k is triangular then $8k+1$ is square. So let k be the triangular number T_n , namely $k = \frac{1}{2}n(n+1)$. Therefore

$$8k + 1 = \frac{1}{2} \times 8n(n+1) + 1 = 4n^2 + 4n + 1 = (2n+1)^2,$$

which is a square.

Conversely, suppose that $8k+1$ is a square so that $8k+1 = r^2$ for some integer r . But $8k+1$ is odd and so r must be odd (because the square of any even integer is even). So $r = 2s+1$, for some integer s , and

$$8k + 1 = (2s+1)^2 = 4s^2 + 4s + 1 = 4s(s+1) + 1,$$

which on solving for k gives $k = \frac{1}{2}s(s+1)$, the triangular number T_s .

Solution to Exercise 2.3

- (a) The n th k -gonal number is the sum of n terms of the arithmetic progression with first term $a = 1$ and common difference $d = k - 2$. So, by the formula for arithmetic series,

$$P(k, n) = \frac{1}{2}n(2 + (n-1)(k-2)).$$

To get the right-hand column of the table of polygonal numbers we put $k = 3, 4, 5, \dots, 8$, giving respectively

$$\frac{1}{2}n(n+1), \quad n^2, \quad \frac{1}{2}n(3n-1), \quad n(2n-1), \quad \frac{1}{2}n(5n-3), \quad n(3n-2).$$

To get the k -gonal numbers in the bottom row of the table we put $n = 1, 2, 3, \dots, 8$, giving respectively

$$1, \quad k, \quad 3(k-1), \quad 2(3k-4), \quad 5(2k-3), \quad 3(5k-8), \quad 7(3k-5), \quad 4(7k-12).$$

(b) Using the formula from part (a), we obtain the following.

$$\begin{aligned}
 P(k-1, n) + P(3, n-1) &= \frac{1}{2}n(2 + (n-1)(k-3)) + \frac{1}{2}(n-1)n \\
 &= \frac{1}{2}n(2 + (n-1)(k-3) + (n-1)) \\
 &= \frac{1}{2}n(2 + (n-1)(k-3+1)) \\
 &= \frac{1}{2}n(2 + (n-1)(k-2)) \\
 &= P(k, n)
 \end{aligned}$$

Solution to Exercise 2.4

(a) Putting $k = 5$, we have

$$Q(5, n) = Q(4, n) + Q(3, n-1).$$

That is, from Table 2.2,

$$\begin{aligned}
 Q(5, n) &= \frac{1}{6}n(n+1)(2n+1) + \frac{1}{6}(n-1)(n)(n+1) \\
 &= \frac{1}{6}n(n+1)(2n+1+n-1) \\
 &= \frac{1}{6}n(n+1)(3n) \\
 &= \frac{1}{2}n^2(n+1).
 \end{aligned}$$

Putting $k = 6$, we have

$$Q(6, n) = Q(5, n) + Q(3, n-1),$$

and so

$$\begin{aligned}
 Q(6, n) &= \frac{1}{2}n^2(n+1) + \frac{1}{6}(n-1)(n)(n+1) \\
 &= \frac{1}{6}n(n+1)(3n+n-1) \\
 &= \frac{1}{6}n(n+1)(4n-1).
 \end{aligned}$$

(b) If $2n^2 \pm 1 = m^2$ then

$$\begin{aligned}
 (nm)^2 &= n^2m^2 \\
 &= n^2(2n^2 \pm 1) \\
 &= \frac{1}{2}2n^2(2n^2 \pm 1) \\
 &= \frac{1}{2}k(k+1), \quad \text{where } k = 2n^2 \text{ when } 2n^2 + 1 \text{ is square,} \\
 &\quad \text{or } k = 2n^2 - 1 \text{ when } 2n^2 - 1 \text{ is square,} \\
 &= T_k.
 \end{aligned}$$

The first three positive values of n for which either $2n^2 + 1$ or $2n^2 - 1$ is square are:

$$\begin{aligned}
 n = 1, \quad 2n^2 - 1 &= 1, \quad \text{giving } T_1 = \frac{1}{2} \times 1 \times 2 = 1; \\
 n = 2, \quad 2n^2 + 1 &= 9, \quad \text{giving } T_8 = \frac{1}{2} \times 8 \times 9 = 36; \\
 n = 5, \quad 2n^2 - 1 &= 49, \quad \text{giving } T_{49} = \frac{1}{2} \times 49 \times 50 = 1225.
 \end{aligned}$$

If you overlooked $n = 1$, the next occurs at $n = 12$ giving $T_{288} = 41\,616$ as a triangular square.

- (c) Any triangular number is of the form $\frac{1}{2}k(k+1)$. If the final digit of such a number was any of 2, 4, 7 or 9 then, by doubling, the final digit of $k(k+1)$ would be 4, 8, 4 or 8 respectively. Now k can take any positive value so its final digit can be any of the ten digits. In each case we can determine the final digit of $k(k+1)$, as follows.

Final digit of k	Final digit of $k+1$	Final digit of $k(k+1)$
0	1	0
1	2	2
2	3	6
3	4	2
4	5	0
5	6	0
6	7	2
7	8	6
8	9	2
9	0	0

This confirms that the final digit of $k(k+1)$ cannot be 4 or 8 and so the final digit of $\frac{1}{2}k(k+1)$ cannot be 2, 4, 7 or 9.

Solution to Exercise 3.1

- (a) (i) The set $\{n \in \mathbb{Z} : |n| > 20\}$ consists of all the integers except those from -20 to 20 inclusive. That is,

$$\{\dots, -23, -22, -21, 21, 22, 23, \dots\}.$$

- (ii) The set $\{n : n = 2m^2, \text{ for some } m \in \mathbb{N}\}$ is the set consisting of those integers that are equal to twice the square of a positive integer, namely

$$\{2, 8, 18, 32, \dots\}.$$

- (b) (i) The set is $\{n : n = 2m - 1, \text{ for some } m \in \mathbb{N}\}$.

We could equally well write this set as $\{n : n = 2m + 1, \text{ for some } m \in \mathbb{Z} \text{ with } m \geq 0\}$.

- (ii) The set is $\{n \in \mathbb{Z} : |n| \leq 100\}$.

Solution to Exercise 3.2

- (a) Let $P(n)$ be the proposition that the formula is true for the natural number n .

Then $P(1)$ is true since

$$1^2 = \frac{1}{6} \times 1(1+1)(2+1).$$

Hence we have the basis for the induction.

For the induction step, assume that $P(k)$ is true, that is,

$$1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{1}{6}k(k+1)(2k+1).$$

Then

$$\begin{aligned}
 & 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2, \quad \text{the LHS of } P(k+1), \\
 &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2, \quad \text{by the induction hypothesis,} \\
 &= \frac{1}{6}(k+1)(2k^2 + k + 6(k+1)) \\
 &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\
 &= \frac{1}{6}(k+1)(k+2)(2k+3) \\
 &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1), \quad \text{the RHS of } P(k+1).
 \end{aligned}$$

This shows that $P(k+1)$ is true and completes the induction step.

Hence, by mathematical induction, the formula is true for all natural numbers n .

- (b) Let $P(n)$ be the proposition that the formula is true for n .

Then $P(1)$ is true since

$$a = \frac{a(r-1)}{r-1}.$$

So we have the basis for the induction.

Now for the induction step. Assume that $P(k)$ is true; that is,

$$a + ar + ar^2 + ar^3 + \cdots + ar^{k-1} = \frac{a(r^k - 1)}{r - 1}.$$

Then

$$\begin{aligned}
 & a + ar + ar^2 + ar^3 + \cdots + ar^{k-1} + ar^k \\
 &= \frac{a(r^k - 1)}{r - 1} + ar^k, \quad \text{by the induction hypothesis,} \\
 &= \frac{a(r^k - 1) + ar^k(r - 1)}{r - 1} \\
 &= \frac{a(r^{k+1} - 1)}{r - 1},
 \end{aligned}$$

which is $P(k+1)$, completing the induction step.

Hence, by mathematical induction, the formula is true for all natural numbers n .

Solution to Exercise 3.3

Let $P(n)$ be the proposition that $L_n < \left(\frac{7}{4}\right)^n$.

We note that $P(1)$ and $P(2)$ are true since

$$L_1 = 1 < \frac{7}{4} \quad \text{and} \quad L_2 = 3 < \left(\frac{7}{4}\right)^2 = \frac{49}{16}.$$

So we have the basis for the induction.

For the induction step (using the Second Principle) suppose that $P(1), P(2), \dots, P(k)$ are all true and consider $P(k+1)$ for $k \geq 2$.

$$\begin{aligned}
 L_{k+1} &= L_k + L_{k-1} \\
 &< \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1}, \quad \text{by the induction hypothesis,} \\
 &= \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4} + 1\right) \\
 &= \left(\frac{7}{4}\right)^{k-1} \left(\frac{11}{4}\right) \\
 &< \left(\frac{7}{4}\right)^{k-1} \left(\frac{7}{4}\right)^2, \quad \text{since } \frac{11}{4} < \frac{49}{16}, \\
 &= \left(\frac{7}{4}\right)^{k+1},
 \end{aligned}$$

which shows that $P(k+1)$ is true.

Hence, by the Second Principle of Mathematical Induction, the proposition is true.

Note that, since the proof of the induction step uses the formula $L_{k+1} = L_k + L_{k-1}$, which holds only for $k \geq 2$, our induction step first deduces the truth of $P(3)$ from that of $P(1)$ and $P(2)$, and then goes on to deduce the truth of $P(4)$, $P(5)$, etc. It does not deduce the truth of $P(2)$ from $P(1)$. Hence we have to show the truth of $P(2)$ separately, which we have done by including it in the basis for the induction.

Solution to Exercise 3.4

(a) (i) Let $P(n)$ be the proposition that the formula is true for n .

$P(1)$ is true, since

$$1^2 = \frac{1}{3} \times 1 \times (4 \times 1^2 - 1).$$

This gives the basis for the induction.

Assume that $P(k)$ is true for some natural number k ; that is,

$$1^2 + 3^2 + 5^2 + \dots + (2k-1)^2 = \frac{1}{3}k(4k^2 - 1).$$

Then

$$\begin{aligned}
 &1^2 + 3^2 + 5^2 + \dots + (2k-1)^2 + (2k+1)^2, \quad \text{the LHS of } P(k+1), \\
 &= \frac{1}{3}k(4k^2 - 1) + (2k+1)^2, \quad \text{by the induction hypothesis,} \\
 &= \frac{1}{3}k(2k-1)(2k+1) + (2k+1)^2 \\
 &= \frac{1}{3}(2k+1)[k(2k-1) + 3(2k+1)] \\
 &= \frac{1}{3}(2k+1)(2k^2 + 5k + 3) \\
 &= \frac{1}{3}(2k+1)(2k+3)(k+1) \\
 &= \frac{1}{3}(k+1)(4k^2 + 8k + 3) \\
 &= \frac{1}{3}(k+1)(4(k+1)^2 - 1), \quad \text{the RHS of } P(k+1),
 \end{aligned}$$

which establishes the truth of $P(k+1)$, and completes the induction step.

Hence, by the Principle of Mathematical Induction, the formula is true for all natural numbers.

(ii) Let $P(n)$ be the proposition that the formula is true for n .

Then $P(1)$ is true since

$$1 = \frac{1}{2} \times 1^2 \times (1 + 1).$$

Assume that $P(k)$ is true; that is,

$$1 + 5 + 12 + 22 + \cdots + \frac{1}{2}k(3k - 1) = \frac{1}{2}k^2(k + 1).$$

Then

$$\begin{aligned} 1 + 5 + 12 + 22 + \cdots + \frac{1}{2}k(3k - 1) + \frac{1}{2}(k + 1)(3k + 2) \\ &= \frac{1}{2}k^2(k + 1) + \frac{1}{2}(k + 1)(3k + 2) \\ &= \frac{1}{2}(k + 1)(k^2 + 3k + 2) \\ &= \frac{1}{2}(k + 1)^2(k + 2), \end{aligned}$$

confirming that $P(k + 1)$ is true and completing the induction step.

The truth of $P(n)$ for all $n \geq 1$ follows by mathematical induction.

(b) Let $P(n)$ be the proposition that the formula is true for n .

$P(1)$ is certainly true since

$$1 \times (1!) = 2! - 1,$$

both sides being equal to 1.

For the induction step, suppose that $P(k)$ is true for some $k \geq 1$. That is,

$$1 \times (1!) + 2 \times (2!) + \cdots + k \times (k!) = (k + 1)! - 1.$$

Then

$$\begin{aligned} 1 \times (1!) + 2 \times (2!) + \cdots + k \times (k!) + (k + 1) \times ((k + 1)!) \\ &= (k + 1)! - 1 + (k + 1)((k + 1)!) \\ &= (k + 1)!(1 + k + 1) - 1 \\ &= (k + 2)! - 1, \end{aligned}$$

which confirms the truth of $P(k + 1)$ and completes the induction step.

The truth of $P(n)$ for all $n \geq 1$ follows by mathematical induction.

(c) We observe that $n!$ increases more rapidly than $6n^2$ and $n!$ exceeds $6n^2$ for the first time when $n = 6$. So we make the conjecture that $n! > 6n^2$ for all $n \geq 6$, and prove it by mathematical induction.

Let $P(n)$ be the proposition that $n! > 6n^2$. Now

$$6! = 720 > 6 \times 6^2 = 216,$$

so $P(6)$ is true, giving us the basis for induction.

Suppose that $P(k)$ is true for some integer $k \geq 6$, that is,

$$k! > 6k^2.$$

On multiplying through by $k + 1$, we get

$$(k + 1)! > 6k^2(k + 1).$$

If we can show that $k^2 \geq k + 1$ it will follow that $(k + 1)! > 6(k + 1)^2$, completing the induction step. But this is easily seen since, for $k \geq 6$,

$$k^2 \geq 6k > 2k = k + k > k + 1,$$

which completes the induction step.

So by the Generalised Principle of Mathematical Induction, $P(n)$ is true for all $n \geq 6$.

(d) Suppose that

$$S = \{k \in \mathbb{Z} : k \geq n_0 \text{ and } P(k) \text{ is false}\}$$

is non-empty. We cannot apply the Well-Ordering Principle directly to this set, as it may not be a subset of $\mathbb{N}$.

Now consider the set T defined by

$$T = \{s - n_0 : s \in S\}.$$

Certainly T is a non-empty set of integers, each of whose elements is greater than or equal to zero. Now, by condition (a), $P(n_0)$ is true so n_0 is not an element of S . Hence zero is not an element of T , and T is a non-empty subset of $\mathbb{N}$.

By the Well-Ordering Principle, T has a least element. We may take this least element of T to be $m - n_0$ for some integer m in S and, by the definition of T , it follows that m is the least element of S .

Furthermore, since $n_0 \notin S$ we know that $m > n_0$, which ensures that the list $P(n_0), P(n_0 + 1), \dots, P(m - 1)$ contains at least one element. By the definition of S it follows that $P(n_0), P(n_0 + 1), \dots, P(m - 1)$ must all be true. But then condition (b') gives that $P(m)$ is true, which contradicts the fact that $m \in S$.

Hence the only assumption made, namely that S is non-empty, must be false. Hence S is empty and so the proposition $P(k)$ is true for all $k \geq n_0$.

Solution to Exercise 4.1

Cubing each of the three given forms that the number can take, and then writing each cube in the form $9n + r$, where $0 \leq r < 9$, gives

$$(3n)^3 = 27n^3 = 9(3n^3) + 0,$$

$$(3n + 1)^3 = 27n^3 + 27n^2 + 9n + 1 = 9(3n^3 + 3n^2 + n) + 1,$$

$$(3n + 2)^3 = 27n^3 + 54n^2 + 36n + 8 = 9(3n^3 + 6n^2 + 4n) + 8.$$

Hence the only possible remainders are 0, 1 and 8.

Solution to Exercise 4.2

(a) The factors of 18 are 1, 2, 3, 6, 9 and 18. The factors of -24 are 1, 2, 3, 4, 6, 8, 12 and 24. (These are the same as the factors of 24.)

The common factors of 18 and -24 are 1, 2, 3 and 6.

- (b) The Division Algorithm tells us that n takes one of the three forms $3k$, $3k + 1$ or $3k + 2$. But n is not a multiple of 3 and so the first of these forms cannot occur.

For $n = 3k + 1$ we get

$$(3k + 1)^2 - 1 = 9k^2 + 6k + 1 - 1 = 3(3k^2 + 2k).$$

For $n = 3k + 2$ we get

$$(3k + 2)^2 - 1 = 9k^2 + 12k + 4 - 1 = 3(3k^2 + 4k + 1).$$

In each case $n^2 - 1$ has remainder zero on dividing by 3.

Solution to Exercise 4.3

- (a) First let m and n be integers such that $\text{hcf}(a, b) = ma + nb$. Then, if c is a multiple of $\text{hcf}(a, b)$, say $c = k \times \text{hcf}(a, b)$, we have

$$c = k(ma + nb) = (km)a + (kn)b,$$

showing that c is an integer combination of a and b .

Remember that 'if, and only if' proofs have two parts.

Conversely, if there are integers x and y such that $c = xa + yb$ then, as $\text{hcf}(a, b)$ divides both a and b , property (e) of Theorem 4.4 confirms that $\text{hcf}(a, b)$ divides $c = xa + yb$.

- (b) Let $d = \text{hcf}(a, b)$. Then, from $d = ma + nb$, we have $1 = ma' + nb'$, where $a = da'$ and $b = db'$. It follows from Lemma 4.9 that $\text{hcf}(m, n) = 1$.
- (c) From $\text{hcf}(a, b) = 1$ and $\text{hcf}(a, c) = 1$ we infer the existence of integers m, n, r and s such that

$$ma + nb = 1 \quad \text{and} \quad ra + sc = 1.$$

Multiplying these two equations together, we get

$$(ma + nb)(ra + sc) = 1,$$

and collating the terms appropriately we get

$$(mar + nbr + msc)a + (ns)bc = 1,$$

which expresses 1 as an integer combination of a and bc . The result then follows from Lemma 4.9.

- (d) There exist integers m, n, r and s such that

$$\text{hcf}(a, b) = ma + nb \quad \text{and} \quad \text{hcf}(ka, kb) = r(ka) + s(kb).$$

But then

$$\begin{aligned} \text{hcf}(ka, kb) &= k(ra + sb) \\ &= k(t \times \text{hcf}(a, b)), \quad \text{for some integer } t, \text{ by part (a) above,} \\ &= t(k \times \text{hcf}(a, b)). \end{aligned}$$

In addition we have

$$\begin{aligned} k \times \text{hcf}(a, b) &= k(ma + nb) \\ &= m(ka) + n(kb) \\ &= u \times \text{hcf}(ka, kb), \quad \text{for some integer } u, \text{ by part (a).} \end{aligned}$$

We now know that each of $\text{hcf}(ka, kb)$ and $k \times \text{hcf}(a, b)$ is a multiple of the other, and so the equality follows from property (c) of Theorem 4.4.

Solution to Exercise 4.4

(a) As $\text{hcf}(a, b) = 1$ there exist integers m and n such that

$$ma + nb = 1.$$

(i) If c divides a then $a = kc$ for some integer k . Substituting for this value of a gives

$$mkc + nb = 1$$

and, as this expresses 1 as an integer combination of b and c , Lemma 4.9 gives $\text{hcf}(b, c) = 1$.

(ii) Our goal is to express 1 as an integer combination of a and $a + b$. This is achieved from the equation $ma + nb = 1$ by careful rearrangement:

$$ma + nb = (m - n)a + n(a + b) = 1.$$

(b) (i) If d divides $3n + 2$ and d divides $5n + 3$ then d divides $5(3n + 2) + (-3)(5n + 3)$. That is, d divides 1. It follows that the only common factor of $3n + 2$ and $5n + 3$ is 1.

(ii) Let $\text{hcf}(n^2 + 3n + 1, 2n + 1) = d$. Then d divides any integer combination of $n^2 + 3n + 1$ and $2n + 1$. We first choose one that eliminates the term in n^2 , namely

$$2(n^2 + 3n + 1) + (-n)(2n + 1) = 5n + 2.$$

So d divides $5n + 2$ and d divides $2n + 1$. Therefore, as before, d divides any integer combination of $5n + 2$ and $2n + 1$. This time we choose one that eliminates the term in n , namely

$$5(2n + 1) + (-2)(5n + 2) = 1.$$

We conclude that $d = 1$.

Solution to Exercise 4.5

Let $\text{lcm}(a, b) = l$ and let m be any common multiple of a and b . Using the Division Algorithm for dividing m by l , there exist integers q and r such that

$$m = lq + r, \quad \text{where } 0 \leq r < l.$$

Rearranging gives

$$r = 1m + (-q)l$$

and, as both m and l are common multiples of a and b , so too is the integer combination r . But l is the least common multiple of a and b , and so we cannot have $0 < r < l$.

Hence $r = 0$, $m = ql$ and so l divides m .

Solution to Exercise 4.6

- (a) Since $\text{hcf}(18, 24) = 6$, $\text{lcm}(18, 24) = \frac{18 \times 24}{6} = 72$.
- (b) The factors of 27 are 1, 3, 9 and 27 and the largest of these that is also a factor of 45 is 9. Therefore $\text{hcf}(27, 45) = 9$ and
 $\text{lcm}(27, 45) = \frac{27 \times 45}{9} = 135$.
- (c) Any common factor of 39 and 40 must divide $40 - 39$. It follows that $\text{hcf}(39, 40) = 1$ and $\text{lcm}(39, 40) = 39 \times 40 = 1560$.

Note that this example illustrates the general result that, for natural numbers a and b ,

$$\text{lcm}(a, b) = ab \text{ if, and only if, } \text{hcf}(a, b) = 1.$$

Solution to Exercise 4.7

- (a) We have

$$12k + 8 = 3(4k + 2) + 2 = 3m + 2,$$

where $m = 4k + 2$ is an integer.

The converse is false since, for example, $5 = 3 \times 1 + 2$ is of the form $3m + 2$ but has remainder 5 on division by 12.

Since 3 divides 12, the remainder when $12k + r$ is divided by 3 is the same as the remainder when r is divided by 3. This will be equal to 2 when $r = 2, 5, 8$ or 11 .

- (b) Any number is necessarily of one of the forms $7k + r$, where $r = 0, 1, 2, 3, 4, 5$ or 6 . Consider the resulting forms for $(7k + r)^2$ and $(7k + r)^3$. Note that

$$(7k + r)^2 = 49k^2 + 14kr + r^2 = 7(7k^2 + 2kr) + r^2$$

and

$$(7k + r)^3 = 343k^3 + 147k^2r + 21kr^2 + r^3 = 7(49k^3 + 21k^2r + 3kr^2) + r^3.$$

Therefore the remainder on dividing $(7k + r)^2$ by 7 is the same as the remainder on dividing r^2 by 7. Similarly, the remainder on dividing $(7k + r)^3$ by 7 is the same as the remainder on dividing r^3 by 7.

$$\begin{array}{ll} 0^2 = 0 = 7 \times 0 + 0 & 0^3 = 0 = 7 \times 0 + 0 \\ 1^2 = 1 = 7 \times 0 + 1 & 1^3 = 1 = 7 \times 0 + 1 \\ 2^2 = 4 = 7 \times 0 + 4 & 2^3 = 8 = 7 \times 1 + 1 \\ 3^2 = 9 = 7 \times 1 + 2 & 3^3 = 27 = 7 \times 3 + 6 \\ 4^2 = 16 = 7 \times 2 + 2 & 4^3 = 64 = 7 \times 9 + 1 \\ 5^2 = 25 = 7 \times 3 + 4 & 5^3 = 125 = 7 \times 17 + 6 \\ 6^2 = 36 = 7 \times 5 + 1 & 6^3 = 216 = 7 \times 30 + 6 \end{array}$$

From the above, we see that the possible remainders on dividing a square by 7 are 0, 1, 2 and 4 and that the possible remainders on dividing a cube by 7 are 0, 1 and 6. So if a number is both a square and a cube then its remainder on division by 7 must be either 0 or 1.

- (c) Let $P(n)$ be the statement that 9 divides $4^n + 6n - 1$.

When $n = 0$, $4^n + 6n - 1 = 0$ and, as this is a multiple of 9, $P(0)$ is true. This gives the basis for induction.

Suppose that $P(k)$ is true for some integer $k \geq 0$; that is, $4^k + 6k - 1 = 9m$ for some integer m . Then

$$\begin{aligned} 4^{k+1} + 6(k+1) - 1 &= 4 \times 4^k + 6(k+1) - 1 \\ &= 4(9m - 6k + 1) + 6(k+1) - 1 \\ &= 36m - 18k + 9 \\ &= 9(4m - 2k + 1), \end{aligned}$$

showing that 9 divides $4^{k+1} + 6(k+1) - 1$, which verifies $P(k+1)$ and completes the induction step.

The result follows by mathematical induction.

- (d) The general result illustrated is that 36 divides $10^n + 8$ for all $n \geq 2$.

The result is true for $n = 2$ since $108 = 3 \times 36$, which is the basis for the induction.

For the induction step suppose that 36 divides $10^k + 8$, for some integer $k \geq 2$. To be precise, suppose that $10^k + 8 = 36r$ for some integer r . Then

$$\begin{aligned} 10^{k+1} + 8 &= 10 \times 10^k + 8 \\ &= 10(36r - 8) + 8 \\ &= 36(10r) - 72 \\ &= 36(10r - 2), \end{aligned}$$

showing that $10^{k+1} + 8$ is divisible by 36, as required.

Hence, by mathematical induction, 36 divides $10^n + 8$ for all integers $n \geq 2$.

- (e) There exist integers m and n such that $am + bn = 1$. Multiplying by c gives

$$m(ac) + (cn)b = c.$$

This expresses c as an integer combination of ac and b and so, by Exercise 4.3(a), c is a multiple of $\text{hcf}(ac, b)$. But, by definition, b is a multiple of $\text{hcf}(ac, b)$ and so $\text{hcf}(ac, b)$ is a common factor of b and c and, in particular,

$$\text{hcf}(ac, b) \leq \text{hcf}(b, c).$$

On the other hand, $\text{hcf}(b, c)$ divides b and $\text{hcf}(b, c)$ divides ac (since it divides c), and so

$$\text{hcf}(b, c) \leq \text{hcf}(ac, b).$$

The equality follows.

- (f) (i) Let $\text{hcf}(2a + b, a + b) = d$. Then, using property (e) of Theorem 4.4,

$$d \mid ((2a + b) - (a + b)), \text{ that is, } d \mid a$$

and

$$d \mid ((-1)(2a + b) + 2(a + b)), \text{ that is, } d \mid b.$$

It follows that d divides $\text{hcf}(a, b)$, and so $d = 1$.

- (ii) Let $\text{hcf}(a + b, a - b) = d$. Then, using property (e) of Theorem 4.4,

$$d \mid ((a + b) + (a - b)), \text{ that is, } d \mid 2a$$

and

$$d \mid ((a + b) - (a - b)), \text{ that is, } d \mid 2b.$$

Hence

$$\begin{aligned} d &\leq \text{hcf}(2a, 2b) = 2 \times \text{hcf}(a, b), \quad \text{by Exercise 4.3(d),} \\ &= 2, \end{aligned}$$

so $d = 1$ or 2 as required.

Solution to Exercise 5.1

$$1092 = 1 \times 777 + 315$$

$$777 = 2 \times 315 + 147$$

$$315 = 2 \times 147 + 21$$

$$147 = 7 \times 21 + 0$$

So $\text{hcf}(1092, 777)$ is equal to the last non-zero remainder, namely 21.

Reversing the equations, we get the following.

$$\begin{aligned} \text{hcf}(1092, 777) &= 21 \\ &= 315 - 2 \times 147 \\ &= 315 - 2 \times (777 - 2 \times 315) \\ &= -2 \times 777 + 5 \times 315 \\ &= -2 \times 777 + 5 \times (1092 - 777) \\ &= 5 \times 1092 - 7 \times 777 \end{aligned}$$

The required integers are $m = 5$ and $n = -7$.

Solution to Exercise 5.2

- (a) The negative coefficient causes no problem if we think of the equation as being $45x + 14(-y) = 7$ and solve for x and $-y$. The Euclidean Algorithm yields the following equations.

$$45 = 3 \times 14 + 3$$

$$14 = 4 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

Reversing the equations, we have

$$1 = 3 - 2$$

$$= 3 - (14 - 4 \times 3)$$

$$= -1 \times 14 + 5 \times 3$$

$$= -1 \times 14 + 5 \times (45 - 3 \times 14)$$

$$= 5 \times 45 - 16 \times 14.$$

Multiplying by 7,

$$7 = 35 \times 45 - 112 \times 14,$$

so that $x = 35$, $-y = -112$ (that is, $y = 112$) is one solution of the equation.

The general solution is

$$x = 35 + 14k, \quad y = 112 + 45k, \quad k \in \mathbb{Z}.$$

The solution with the least positive value of x is given by $k = -2$, namely $x = 7$, $y = 22$.

Note that the general solution can therefore be written as

$$x = 7 + 14k, \quad y = 22 + 45k, \quad k \in \mathbb{Z}.$$

- (b) If x is the number of 50p stamps bought and y is the number of 60p stamps then the total amount spent is $50x + 60y$ pence. Hence $50x + 60y = 3000$, and, as we are not allowed fractions of stamps, our task is to solve this in integers.

We first note that $\text{hcf}(50, 60) = 10$, and, since 10 divides 3000, there are solutions. Dividing the whole equation by 10 gives $5x + 6y = 300$. It is not difficult to ‘spot’ one solution of this equation. As 5 divides 300 we see that $x = 60$, $y = 0$ is a solution. Theorem 5.4 then gives the general solution:

$$x = 60 - 6k, \quad y = 0 + 5k, \quad k \in \mathbb{Z}.$$

We seek the particular solution in which $|x - y|$ is as small as possible; that is, we want to minimise $|60 - 11k|$. But $11k$ is nearest to 60 when $k = 5$, giving $x = 30$, $y = 25$ as the required solution.

The expression for y comes from our previous general solution, which gave $-y = -112 - 45k$. If you substitute back into the original equation, note that these ‘added’ terms do cancel.

You can, of course, use the Euclidean Algorithm, but do look out for shortcuts.

Solution to Exercise 5.3

(a) Since we can write

$$143 = 8 \times 17 + 7$$

$$17 = 2 \times 7 + 3$$

$$7 = 2 \times 3 + 1$$

$$3 = 3 \times 1 + 0,$$

it follows that

$$\begin{aligned} \text{hcf}(143, 17) &= 1 \\ &= 7 - 2 \times 3 \\ &= 7 - 2(17 - 2 \times 7) \\ &= -2 \times 17 + 5 \times 7 \\ &= -2 \times 17 + 5(143 - 8 \times 17) \\ &= 5 \times 143 - 42 \times 17. \end{aligned}$$

Therefore $x = -42$, $y = 5$ is one solution. The general solution is therefore

$$x = -42 + 143k, \quad y = 5 - 17k, \quad k \text{ any integer.}$$

The particular solution in which x takes its least positive value occurs when $k = 1$, and is $x = 101$, $y = -12$.

(b) Since we can write

$$158 = 2 \times 57 + 44$$

$$57 = 1 \times 44 + 13$$

$$44 = 3 \times 13 + 5$$

$$13 = 2 \times 5 + 3$$

$$5 = 1 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0,$$

it follows that

$$\begin{aligned} \text{hcf}(158, 57) &= 1 \\ &= 3 - 1 \times 2 \\ &= 3 - (5 - 1 \times 3) \\ &= -1 \times 5 + 2 \times 3 \\ &= -1 \times 5 + 2(13 - 2 \times 5) \\ &= 2 \times 13 - 5 \times 5 \\ &= 2 \times 13 - 5(44 - 3 \times 13) \\ &= -5 \times 44 + 17 \times 13 \\ &= -5 \times 44 + 17(57 - 44) \\ &= 17 \times 57 - 22 \times 44 \\ &= 17 \times 57 - 22(158 - 2 \times 57) \\ &= -22 \times 158 + 61 \times 57. \end{aligned}$$

Therefore $x = -22$, $y = -61$ is one solution of the Diophantine equation $158x - 57y = 1$ and, multiplying by 7, $x = -154$, $y = -427$ is one solution of the equation $158x - 57y = 7$.

The general solution of the latter equation is therefore given by

$$x = -154 + 57k, \quad y = -427 + 158k, \quad k \text{ any integer.}$$

When $k \geq 3$, x and y are both positive, the least positive solution being $x = 17$, $y = 47$. The set of all positive solutions is

$$x = 17 + 57s, \quad y = 47 + 158s, \quad s \geq 0.$$

- (c) First notice that we can divide the equation $39x + 27y = 3$ through by 3, which gives us

$$13x + 9y = 1.$$

We now use the Euclidean Algorithm on 13 and 9:

$$13 = 1 \times 9 + 4$$

$$9 = 2 \times 4 + 1$$

$$4 = 4 \times 1 + 0.$$

Thus, we have

$$\begin{aligned} \text{hcf}(9, 13) &= 1 \\ &= 9 - 2 \times 4 \\ &= 9 - 2 \times (13 - 9) \\ &= 3 \times 9 - 2 \times 13. \end{aligned}$$

Therefore $x = -2$ and $y = 3$ is one solution of the Diophantine equation $13x + 9y = 1$, and therefore also one solution of the original Diophantine equation $39x + 27y = 3$.

Applying Theorem 5.4, the general solution to $39x + 27y = 3$ is therefore

$$x = -2 + 9k, \quad y = 3 - 13k, \quad k \text{ any integer.}$$

- (d) Suppose that x 2p coins, y 10p coins and z 50p coins are used. Then, since the total value is £6,

$$2x + 10y + 50z = 600.$$

Furthermore, as the total number of coins used is 100,

$$x + y + z = 100.$$

Substituting $2x = 200 - 2y - 2z$ into the former equation gives $200 + 8y + 48z = 600$, which simplifies to

$$y + 6z = 50.$$

One solution of this Diophantine equation may be spotted immediately, namely $y = 50$, $z = 0$. Hence the general solution is

$$y = 50 - 6k, \quad z = k, \quad k \in \mathbb{Z}.$$

Now as $x = 100 - y - z$, we seek non-negative solutions from

$$x = 50 + 5k, \quad y = 50 - 6k, \quad z = k, \quad k \in \mathbb{Z}.$$

Choosing $k \geq 0$ guarantees that x and z are non-negative and $k \leq 8$ keeps y non-negative. Hence there are nine solutions corresponding to $k = 0$ to 8 inclusive. These are given in the following table.

k	x	y	z
0	50	50	0
1	55	44	1
2	60	38	2
3	65	32	3
4	70	26	4
5	75	20	5
6	80	14	6
7	85	8	7
8	90	2	8

Chapter 2

Prime numbers

Introduction

The fact that some numbers break up into factors, such as $12 = 3 \times 4$, whereas others cannot be broken up, such as 13, must surely have intrigued most people at some stage of their mathematical education. The numbers that cannot be broken up, such as

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, $\dots$,

are called the *primes*, and we will rapidly discover that they form a central concept in any study of the theory of numbers. Almost every investigation involves them in one way or another.

As numbers get larger it appears that the likelihood of having factors increases, which might make you wonder whether there is a largest prime. If so, how many primes are there? In Book IX of *Elements*, Euclid showed that in fact the sequence of primes does not end; there are infinitely many primes. Euclid's proof of this fact, which we reproduce in this chapter, has universal appeal because of its elegance and simplicity.

Since Euclid, a prodigious amount of effort has been expended on producing more extensive tables of prime numbers, and the search to find larger and larger primes has continued unabated. The first significant record of a table of primes is due to Fibonacci (*c.*1170–*c.*1250) who, in the year 1202, listed primes up to 100. By 1603 Pietro Cataldi (1548–1626) had listed all primes up to 750. Developments followed closely after that and by the end of the eighteenth century, lists of all primes up to one million were recorded. The arrival of computers accelerated discoveries to such an extent that it is difficult to keep track of the largest known prime. By the early twenty-first century, numbers such as $2^{57\,885\,161} - 1$, which when written out has 17 425 170 digits, had been proved by computer to be prime.

How would we go about producing a list of all primes up to, say, 1000? A simple-minded approach would be to take each integer in turn and check its divisibility by each smaller positive integer, concluding that the number is prime if none of the smaller positive integers (other than 1) divides it. However, the amount of calculation involved in this approach makes it impractical, even with the benefit of a number of shortcuts that are available. An early Greek mathematician, Eratosthenes (276–194 BC), devised a superior approach, which you will meet and use in this chapter.

Since the dawn of mathematical history, problems involving primes and how to classify them have fascinated and attracted the attention of the greatest mathematical minds. How many primes p are there for which $p + 2$ is also prime? Can every even integer from 4 onwards be written as the sum of two primes? Is there a maximum length for a sequence of consecutive integers none of which is prime? Throughout this chapter we look at classical problems, including these, provide answers to some and discuss others which, despite considerable numerical evidence in support of their validity, remain unsolved in spite of numerous attempts at proofs over the years.

How is the infinite set of primes distributed amongst the set of all integers? Could, for example, every sixth integer from 5 onwards be prime? This arithmetic progression begins

5, 11, 17, 23, 29, ...;

the first five members of this sequence are prime but the next, 35, is not. Can any arithmetic progression consist of primes alone? Can an arithmetic progression contain infinitely many primes? We will look at some problems in this area, providing answers to questions concerning the presence of primes, first in arithmetic progressions and then in other sequences.

In the final section of the chapter we introduce and discuss another intriguing sequence of integers about which many questions can be answered: the *Fibonacci sequence*. As well as being of interest for its own sake, the Fibonacci sequence will enable you to gain practice in applying results and techniques developed elsewhere in the first two chapters, in particular those concerning divisibility properties.

Chapter guide

This chapter is divided into five sections. The first three are of approximately equal length, and form the core material in this chapter. Section 4 is less technical, and shows you how number theory is still a very active area of research for mathematicians. Finally, Section 5 shows you some connections between prime numbers and the Fibonacci sequence.

1 The primes

This chapter begins by exploring some of the basic properties of the prime numbers.

1.1 Basic properties

We begin with the key definition.

Definition 1.1 Prime numbers

An integer n , where $n \geq 2$, is said to be **prime** if it has no positive factor other than itself and 1. Otherwise n is said to be **composite**.

Notice that we have excluded consideration of 0 and the negative integers from these definitions; we will not be concerned with the primality or otherwise of non-positive integers. Notice also that the integer 1 is classified neither as prime nor as composite. As the composite integers are essentially those that can be broken down into products of at least two non-trivial (that is, not itself and 1) positive factors, it is natural to

exclude 1 from the composite integers. On the other hand, we do not want to list 1 amongst the primes for a variety of reasons. For example, if 1 were to be considered as a prime,

$$6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3$$

would be three (of infinitely many) different ways of expressing 6 as a product of primes. Excluding 1 from the list of primes enables us to express any integer greater than or equal to 2 as a *unique* product of primes. This result, which we will prove shortly, is of great importance in the study of number theory.

By a product we mean any number of integers multiplied together, including the possibility of a single integer on its own, such as 2.

Is there an efficient way of determining whether a given integer is prime? For example, is 211 prime or is it composite? If we can spot an integer in the range 2 to 210 that divides 211 then we can conclude immediately that 211 is composite. On the other hand, to show that 211 is prime there are a lot of potential factors to be eliminated. Do we have to test division by all the numbers in the range 2 to 210? Fortunately we do not. The following two results show that the list of potential factors can be drastically reduced. The first of these results appeared in Book VII of Euclid's *Elements*.

Proposition 1.2

Each integer $n \geq 2$ is divisible by some prime number.

If n is prime then n is a prime factor of itself.

Proof Preparing for a proof by mathematical induction (using the Second Principle), let $P(n)$ be the statement that the integer $n \geq 2$ is divisible by some prime number.

The statement $P(2)$ is certainly true, since 2 divides 2 and 2 is prime, and this provides the basis for the induction.

For the induction step suppose that for some integer $k \geq 2$, each of $P(2), P(3), \dots, P(k)$ is true; that is, suppose that each of the integers $2, 3, \dots, k$ is divisible by some prime. Now consider the next integer, $k + 1$. Either $k + 1$ is prime or it is composite. If it is a prime, it is divisible by the prime $k + 1$ itself. If it is composite, then $k + 1 = rs$, where r and s are integers with $2 \leq r \leq k$, whereupon the induction hypothesis tells us that there is some prime p that divides r . But then p divides r and r divides $k + 1$ and so p divides $k + 1$. In either case we conclude that $k + 1$ is divisible by some prime, confirming the truth of $P(k + 1)$.

The result follows by mathematical induction. ■

The next result determines a limit to the number of divisions one has to make in order to decide whether a given integer $n \geq 2$ is prime or not.

Proposition 1.3

If the integer $n \geq 2$ is composite, then it is divisible by some prime $p \leq \sqrt{n}$.

Proof As n is composite we can write $n = ab$, where a and b are integers with $2 \leq a \leq b$. Now we cannot have $a > \sqrt{n}$, for that would imply $b > \sqrt{n}$ and the product ab would exceed n . So $a \leq \sqrt{n}$. At this point we can invoke Proposition 1.2, which guarantees the existence of a prime p dividing a (and therefore dividing n). As $p \leq a \leq \sqrt{n}$, p suffices as the required prime. ■

This proposition can be applied to the question of whether 211 is composite. The prime numbers that are less than $\sqrt{211}$ are 2, 3, 5, 7, 11 and 13, and so if 211 is composite it must be divisible by one of these primes. However, straightforward division shows that this is not the case: 211 has remainder 1 when divided by each of 2, 3, 5 and 7, remainder 2 on division by 11 and remainder 3 on division by 13. Hence 211 is prime.

Exercise 1.1

- (a) Which, if any, of the integers 111, 113, 115 and 117 is prime?
- (b) To test whether or not 499 is a prime, for which numbers is it sufficient to check divisibility?

The problem of how to find the primes up to a given integer is tackled in the next subsection.

1.2 The sieve of Eratosthenes

Eratosthenes devised a relatively simple way of listing all the primes up to some number. The method is illustrated for primes up to 100 in Figure 1.1. It works as follows. Write down in order all the natural numbers from 2 up to the chosen limit, 100 in this case. The first number 2 is prime, so we ring it, and then cross out every second number after 2 in the list. These are the non-trivial multiples of 2 (and therefore composite) and are shown crossed out with a horizontal bar in the figure. Having completed this task we return to the number 2. The first number following 2 that is not crossed out is 3, so we ring it as being prime, and proceed to cross out (with a \) every third number following 3, if not already crossed out. Returning to 3, the first number after 3 that is not crossed out is 5, so we ring it as being prime, and cross out (with a /) every fifth number after it, if not already crossed out. Continuing in this way, 7 is ringed next and every seventh number after it is crossed out (with a X).

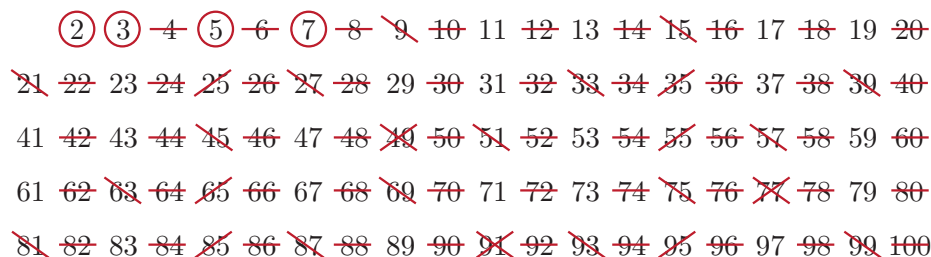


Figure 1.1 Sieving the primes up to 100

The next uncrossed number is the prime 11, but as 11 exceeds $\sqrt{100}$ it turns out that we are finished. All multiples of 11, and, with the same reasoning, multiples of larger primes, must already have been crossed out because any number in the range 2 to 100 that is divisible by 11 is, by Proposition 1.3, also divisible by a prime less than $\sqrt{100}$, and so is a multiple of one of the already ringed primes. We can therefore now ring all the uncrossed numbers in the knowledge that they complete the primes up to 100.

To extend the list of primes beyond 100 we do not have to begin the sieve again. For instance, to pick up the primes in the range 101 to 140 we know that it is a matter of crossing out from a list of these 40 numbers the multiples of each of the primes up to $\sqrt{140}$; that is, we cross out the first multiple of 2, namely 102, and every second number, then the first multiple of 3 (also 102) and every third number, and similarly for primes 5, 7 and 11. Figure 1.2 shows the extension with the one occurring multiple of 11 crossed out (with a $\sim$). The numbers not crossed out are the primes.

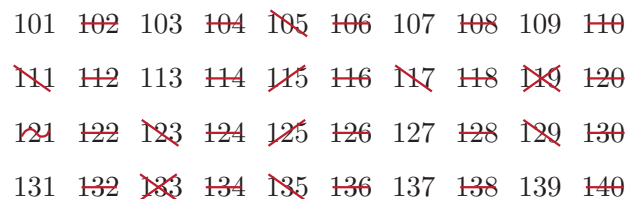


Figure 1.2 Sieving the primes in the range 101 to 140

Exercise 1.2

Extend the sieve to find all primes up to 200.

1.3 The Fundamental Theorem of Arithmetic

Any composite integer can be expressed, possibly in many ways, as a product of factors. For instance, observing that 11 divides 660, we may express the latter as 11×60 . Now the factor 60 is composite, so it may be broken down further into, for example, 4×15 , so that $660 = 11 \times 4 \times 15$. The factors 4 and 15 are each composite, so they can be broken down further. Indeed, by continuing to break down any composite factor in this way, we can eventually express the original number as a product of primes. Figure 1.3 shows three ways in which 660 can be broken down to its prime factors.

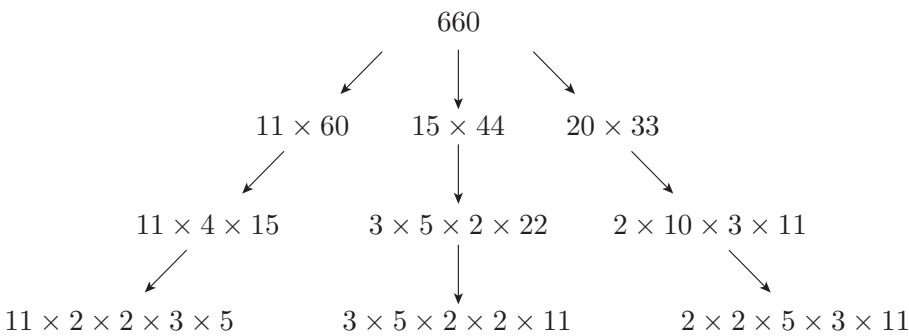


Figure 1.3 Expressing 660 as a product of primes

What is noticeable is that in all these ways of breaking down 660, we end up with the same product of primes; the order in which they are written varies, but in all cases $660 = 2 \times 2 \times 3 \times 5 \times 11$. Our next goal is to show that every integer greater than 1 is expressible as a product of primes in a unique way (except for the order in which the primes are written) – but on the way we will need some divisibility properties involving primes.

First we record one simple property, which will come up frequently, concerning highest common factors. Suppose that p is prime and n is any integer. What can we say about $\text{hcf}(n, p)$? As the only factors of prime p are p itself and 1, $\text{hcf}(n, p)$ has just the two possible values, namely p and 1. Now $\text{hcf}(n, p)$ takes value p precisely when p divides n . Hence we have the following property.

The value of $\text{hcf}(n, p)$

If p is a prime and n is any integer, then

$$\text{hcf}(n, p) = \begin{cases} p, & \text{if } p \text{ divides } n, \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 1.4, which follows below, is a consequence of Euclid's Lemma (Theorem 4.12 of Chapter 1). If a prime p divides a product of numbers then it must divide one of those numbers.

Theorem 1.4 *Euclid's Lemma for prime factors*

If p is prime and p divides the product $a_1 a_2 \cdots a_n$ then p divides a_i , for some integer i , where $1 \leq i \leq n$.

Proof We prove the result by mathematical induction on the number of terms in the product. With that goal in mind let $P(n)$ be the statement of the theorem.

We have the basis for induction since $P(1)$ is trivially true, for it states that if p divides a_1 , then p divides a_1 .

Heading for the induction step, suppose that $P(k)$ is true for some integer $k \geq 1$, that is, if p divides the product of any k integers then p divides one of them. Now consider any product of $k + 1$ integers that is divisible by p , say

$$p \mid a_1 a_2 \cdots a_k a_{k+1}.$$

Either p divides a_{k+1} or it does not. If p divides a_{k+1} we are finished. If p does not divide a_{k+1} then $\text{hcf}(p, a_{k+1}) = 1$. Since p divides the product $(a_1 a_2 \cdots a_k) a_{k+1}$ and $\text{hcf}(p, a_{k+1}) = 1$ we conclude, by Euclid's Lemma (Theorem 4.12 of Chapter 1), that p divides $a_1 a_2 \cdots a_k$. But then, by the induction hypothesis, p divides a_i for some i , where $1 \leq i \leq k$.

Putting the two possibilities together, either p divides a_{k+1} or p divides a_i for some i , where $1 \leq i \leq k$, which verifies that $P(k + 1)$ is true. Hence, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers. ■

One consequence of Theorem 1.4 merits recording, as follows.

Corollary 1.5 *to Euclid's Lemma for prime factors*

If $p, p_1, p_2, \dots, p_n$ are primes such that

$$p \mid p_1 p_2 \cdots p_n,$$

then $p = p_i$ for some i , where $1 \leq i \leq n$.

Proof Theorem 1.4 tells us that p divides p_i for some i , where $1 \leq i \leq n$. But the only factors of p_i are 1 and p_i , and as 1 is not a prime, it follows that $p = p_i$. ■

The following worked exercise makes use of these results.

Worked Exercise 1.6

Let p be prime and a and b be integers. Show that:

- (a) if p divides a^n , then p^n divides a^n
- (b) if $\text{hcf}(a, b) = p$, then $\text{hcf}(a^n, b^n) = p^n$.

Solution

- (a) Using Theorem 1.4 with $a_1 = a_2 = \cdots = a_n = a$, we deduce immediately that if p divides a^n then p divides a . Hence $a = pr$, for some integer r . Raising both sides of this equation to the power n gives $a^n = p^n r^n$, which tells us that p^n divides a^n .
- (b) If $\text{hcf}(a, b) = p$, there exist integers r and s such that $a = pr$ and $b = ps$, with $\text{hcf}(r, s) = 1$. But then

$$\begin{aligned}\text{hcf}(a^n, b^n) &= \text{hcf}(p^n r^n, p^n s^n) \\ &= p^n \text{hcf}(r^n, s^n), \quad \text{by Exercise 4.3(d) of Chapter 1.}\end{aligned}$$

It remains to show that $\text{hcf}(r^n, s^n) = 1$.

Suppose q is a prime that divides $\text{hcf}(r^n, s^n)$. Then q divides r^n and q divides s^n . As we saw in part (a), this implies that q divides r and q divides s , so that q divides $\text{hcf}(r, s)$. But $\text{hcf}(r, s) = 1$, contradicting the existence of such a prime q .

Hence $\text{hcf}(r^n, s^n) = 1$, which completes the proof.

When proving results involving two integers, it is sometimes useful, as here, to divide each by their hcf and then work with the resulting integers, which are coprime by Proposition 4.10 of Chapter 1.

We are just about ready for our main result of this section, but first a word about notation. Earlier we saw several ways of expressing 660 as a product of primes, the only difference between the expressions being the order in which the primes were written. Conventionally, when writing a number down as a product of its prime factors, we arrange the primes in ascending order with like primes collected together as a power. For instance, we write 660 as

$$660 = 2^2 \times 3 \times 5 \times 11.$$

This convention removes the ambiguity of ordering and, as we are about to see, renders a unique representation of the integer as a product of its prime factors. We refer to this as the **prime decomposition** of the integer.

Exercise 1.3

Give the prime decompositions of each of the integers 168, 226 and 36 000.

Theorem 1.7 *The Fundamental Theorem of Arithmetic*

Any integer $n \geq 2$ can be written uniquely in the form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where p_i , $i = 1, \dots, r$, are primes with $p_1 < p_2 < \cdots < p_r$ and each k_i , $i = 1, \dots, r$, is a natural number.

As its name suggests, this theorem is central to many investigations in number theory.

Proof We prove the theorem in two parts. First, we show the *existence* of such a decomposition, that is, we show that n can be expressed as such a product of primes. Second, we show that the prime decomposition obtained is *unique*.

Existence

With proof by mathematical induction in mind, let $P(n)$ be the proposition that n can be expressed as a product of primes. We need to show that $P(n)$ is true for all $n \geq 2$.

Now $P(2)$ is certainly true, since 2 is a prime, and so we have the basis for the induction.

Suppose that, for some integer $k \geq 2$, $P(2), P(3), \dots, P(k)$ are all true. That is, each of $2, 3, \dots, k$ can be written as a product of primes. Now consider the integer $k + 1$. By Proposition 1.2, $k + 1$ is divisible by some prime p and so we may write $k + 1 = pr$, for some integer r . If $r = 1$, $k + 1$ is a prime and we are done. If $r > 1$ then, as $r < k + 1$, the induction hypothesis tells us that r is a product of primes, whereupon $k + 1 = pr$ is also a product of primes. It follows therefore that $P(k + 1)$ is true.

Hence, by the Second Principle of Mathematical Induction, $P(n)$ is true for all integers $n \geq 2$.

Uniqueness

Suppose that some integer $n \geq 2$ has two representations as a product of primes, say,

$$\begin{aligned} n &= p_1 p_2 \cdots p_r, & \text{where } p_1 \leq p_2 \leq \cdots \leq p_r, \\ &= q_1 q_2 \cdots q_s, & \text{where } q_1 \leq q_2 \leq \cdots \leq q_s. \end{aligned}$$

Note that in these expressions for n we have kept the primes separate rather than collecting them in powers.

Now p_1 divides n and so p_1 divides the product $q_1 q_2 \cdots q_s$. By the Corollary to Euclid's Lemma for prime factors, this gives $p_1 = q_j$ for some $1 \leq j \leq s$. As $q_1 \leq q_j$ we conclude that $q_1 \leq p_1$. But there is symmetry between the p s and q s. So similarly we argue that since q_1 divides n , we have $q_1 = p_i$ for some $1 \leq i \leq r$, which leads to $p_1 \leq q_1$. Combining the two inequalities gives $p_1 = q_1$.

Since p_1 divides n we have $n = p_1 n_1$ for some integer n_1 . Hence

$$n_1 = p_2 \cdots p_r = q_2 \cdots q_s,$$

and a repetition of the argument gives $p_2 = q_2$. Then, putting $n = p_1 p_2 n_2$, we get

$$n_2 = p_3 \cdots p_r = q_3 \cdots q_s,$$

giving $p_3 = q_3$.

We can continue in this way, cancelling equal primes from the left of the two products.

If $r < s$ then we obtain $p_i = q_i$ for $1 \leq i \leq r$ and we are left with

$$1 = q_{r+1} \cdots q_s.$$

This is a contradiction, since the q_i are primes. The assumption that $r > s$ leads to a similar contradiction. Hence $r = s$ and the proof of the uniqueness of the prime decomposition is complete. ■

Exercise 1.4

- (a) Show that the integer $n > 1$ with prime decomposition $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is a square if, and only if, each of the exponents k_i is even.
- (b) Use the identity $n^3 - 1 = (n - 1)(n^2 + n + 1)$ to prove that the only prime of the form $n^3 - 1$ is 7.

Exercise 1.5

- (a) Find the prime decomposition of 20!
- (b) Given that p and q are distinct primes such that their product pq divides a^n , prove that $(pq)^n$ divides a^n .
- (c) Prove that the only prime p for which $3p + 1$ is a square is $p = 5$.
- (d) Show that for any prime p , $8p - 1$ and $8p + 1$ cannot both be prime.
Hint: use the fact that p must be either equal to 3 or of one of the forms $3k + 1$ or $3k + 2$.
- (e) Let $p \geq 5$ be prime. Show that the remainder on dividing p by 12 must be one of 1, 5, 7 or 11. Hence prove that if $p \geq q \geq 5$ are primes then $24 \mid (p^2 - q^2)$.
- (f) Prove (as Cataldi did in 1588) that if a is a natural number and $n \geq 2$ such that $a^n - 1$ is prime then $a = 2$ and n is prime.

Hint: consider the factorisation

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

2 The prime decomposition of integers

This section uses the Fundamental Theorem of Arithmetic to explore prime decompositions of integers.

2.1 The prime decomposition of factors

When the prime decomposition of an integer is given, it is a simple matter to obtain all its factors.

Remember that we consider only *positive* factors.

Exercise 2.1

Given that $252 = 2^2 \times 3^2 \times 7$, write down as many factors as you can find of 252, expressing each one in its prime decomposition. Can you formulate a conjecture about the set of all factors of 252?

One of the factors of 252 is 1, which does not have a prime decomposition. For convenience we define the prime decomposition of 1 to be 1 itself.

The observations in the solution to Exercise 2.1 lead to the following generalisation.

Proposition 2.1 *Factors of an integer*

Let n be an integer greater than 1, with prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

Then the set of all factors of n is the set of integers

$$\left\{ p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r} : 0 \leq h_i \leq k_i \text{ for } i = 1, 2, \dots, r \right\}.$$

Proof Certainly each integer in the given set is a factor of n because $k_i - h_i \geq 0$ for each i and

$$n = \left(p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r} \right) p_1^{k_1 - h_1} p_2^{k_2 - h_2} \cdots p_r^{k_r - h_r}.$$

Our task now is to show that the integers in the given set, which are distinct by the uniqueness of prime decomposition, are the *only* factors of n . To that end, let $d > 1$ be a factor of n and let p be a prime factor of d . Since p divides d and d divides n we know that p divides n . Therefore, by the Corollary to Euclid's Lemma for prime factors, $p = p_i$ for some i , where $1 \leq i \leq r$. It follows therefore that the only primes dividing d come from the set $\{p_i : 1 \leq i \leq r\}$. Hence we can write $d = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$, where each h_i is a non-negative integer.

Finally, to show $h_i \leq k_i$ we utilise the fact that d divides n and that, as a consequence, $p_i^{h_i}$ divides n . As $p_1, p_2, \dots, p_r$ are distinct primes, the Corollary to Euclid's Lemma for prime factors confirms that p_1 does not divide $p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$. Hence $\text{hcf}(p_1^{h_1}, p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}) = 1$ and, coupled with the fact that $p_1^{h_1}$ divides $n = p_1^{k_1} (p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r})$, Euclid's Lemma shows

that $p_1^{h_1}$ divides $p_1^{k_1}$, the latter amounting to $h_1 \leq k_1$. The same argument shows that $h_2 \leq k_2, \dots, h_r \leq k_r$. ■

Exercise 2.2

Let $m = 3^3 \times 5 \times 17^2$ and $n = 2 \times 3^2 \times 7 \times 17^4$.

- (a) How many (positive) factors does m have? How many does n have?
- (b) List the common factors of m and n .
- (c) Determine the prime decompositions of $\text{hcf}(m, n)$ and of $\text{lcm}(m, n)$.

Let us look generally at the problem of determining $\text{hcf}(m, n)$ and $\text{lcm}(m, n)$ when the prime decompositions of m and n are at hand. We may suppose that

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{and} \quad n = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r},$$

where $p_1, p_2, \dots, p_r$ are the primes that divide either m or n . This means that what we have written here are not necessarily the prime decompositions; to get the same primes listed for both m and n it may be necessary to include some with exponent 0. For example, if $m = 42 = 2 \times 3 \times 7$ and $n = 35 = 5 \times 7$, we might write

$$m = 2^1 3^1 5^0 7^1, \quad n = 2^0 3^0 5^1 7^1.$$

A factor of m is an integer

$$d = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r},$$

where $0 \leq h_i \leq k_i$ for each $i = 1, 2, \dots, r$. Also, d divides n if, and only if, $h_i \leq l_i$ for each $i = 1, 2, \dots, r$. Combining these two conditions: d is a common factor of m and n if, and only if, $0 \leq h_i \leq \min\{k_i, l_i\}$ for each $i = 1, 2, \dots, r$. For its greatest value d requires the largest possible exponent for each of its primes, and therefore we have the following result.

Prime decomposition of $\text{hcf}(m, n)$

If $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ then

$$\text{hcf}(m, n) = p_1^{\min\{k_1, l_1\}} p_2^{\min\{k_2, l_2\}} \cdots p_r^{\min\{k_r, l_r\}}.$$

In words, the largest prime powers dividing $\text{hcf}(m, n)$ are obtained by raising each prime that divides either m or n to the power that is the smaller of its exponents in m and n . To write $\text{hcf}(m, n)$ in prime decomposition, each resulting term $p_i^{\min\{k_i, l_i\}}$ in which the exponent $\min\{k_i, l_i\}$ is 0 is removed from the expression. If $\min\{k_i, l_i\} = 0$ for each $i = 1, 2, \dots, r$, then $\text{hcf}(m, n) = 1$.

If a and b are integers, then $\min\{a, b\}$ denotes the smaller of a and b .

A corresponding result for $\text{lcm}(m, n)$ is readily obtained from the formula relating $\text{lcm}(m, n)$ to $\text{hcf}(m, n)$:

$$\begin{aligned}\text{lcm}(m, n) &= \frac{mn}{\text{hcf}(m, n)} = \frac{(p_1^{k_1} \cdots p_r^{k_r})(p_1^{l_1} \cdots p_r^{l_r})}{p_1^{\min\{k_1, l_1\}} \cdots p_r^{\min\{k_r, l_r\}}} \\ &= p_1^{k_1 + l_1 - \min\{k_1, l_1\}} \cdots p_r^{k_r + l_r - \min\{k_r, l_r\}}.\end{aligned}$$

Now for any two integers k and l ,

$$k + l - \min\{k, l\} = \max\{k, l\}.$$

This follows since $\min\{k, l\}$ is the smaller of k and l , and subtracting the smaller of k and l from $k + l$ leaves the larger. Therefore we have the following result.

If a and b are integers, then $\max\{a, b\}$ denotes the larger of a and b .

Prime decomposition of $\text{lcm}(m, n)$

If $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ then

$$\text{lcm}(m, n) = p_1^{\max\{k_1, l_1\}} p_2^{\max\{k_2, l_2\}} \cdots p_r^{\max\{k_r, l_r\}}.$$

In words, the prime decomposition of $\text{lcm}(m, n)$ is obtained by raising each prime that divides either m or n to the larger of its exponents in m and n .

Exercise 2.3

If $m = 3^3 \times 5^3 \times 11 \times 19$ and $n = 2 \times 3^2 \times 7 \times 11$, write down the prime decompositions of $\text{hcf}(m, n)$ and $\text{lcm}(m, n)$.

2.2 The τ function

From the prime decomposition of an integer n , Proposition 2.1 demonstrates how to list the factors of n . As a consequence, this proposition tells us exactly how many factors the integer n has. The number of (positive) factors of an integer is used to define a function, denoted by the Greek letter τ .

τ is the Greek letter ‘tau’. We will encounter Greek letters throughout this module, and a complete list of them is given in the *Handbook*.

Definition 2.2 The τ function

For any integer $n \geq 1$, $\tau(n)$ is defined to be the number of distinct factors of n , including 1 and n .

Notice that $\tau(1) = 1$.

To determine the value of $\tau(n)$ from the prime decomposition of n involves little more than some elementary arithmetic.

Proposition 2.3 *The formula for $\tau(n)$*

For any integer $n \geq 2$, with prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

we have

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1).$$

Proof We have established that any factor d of $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ has prime decomposition $p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$, where $0 \leq l_i \leq k_i$ for each $i = 1, 2, \dots, r$. There are $k_1 + 1$ choices for l_1 , $k_2 + 1$ choices for $l_2, \dots$, and $k_r + 1$ choices for l_r . This makes $(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$ choices in all, and, because of the uniqueness of prime decomposition, each of these choices results in a distinct factor. ■

Worked Exercise 2.4

Find all integers less than 100 that have exactly 10 factors.

Solution

If $\tau(n) = 10$, then $(k_1 + 1)(k_2 + 1) \cdots (k_r + 1) = 10$, where the positive integers k_i are the exponents in the prime decomposition of n . There are only two ways that 10 can be expressed as the product of integers greater than 1, namely 2×5 and 10 . In the former case $k_1 = 1$ and $k_2 = 4$, giving $n = p_1 p_2^4$, and in the latter case $k_1 = 9$, giving $n = p_1^9$.

Notice that in writing $n = p_1 p_2^4$ here, we do not know that $p_1 < p_2$, and so the order of the primes is not necessarily as it should be in the prime decomposition. In answering questions such as this we will be lax about writing primes in ascending order.

There are two numbers of the form $p_1 p_2^4$ that do not exceed 100, namely $3 \times 2^4 = 48$ and $5 \times 2^4 = 80$. The smallest number of the form p_1^9 is $2^9 = 512$, so all numbers of this form exceed 100. Hence the only possibilities are 48 and 80.

Exercise 2.4

Find the smallest integer that has exactly 24 factors.

Exercise 2.5

- (a) Let $m = 2^3 \times 3^2 \times 7 \times 11$ and $n = 3344$. Determine the prime decomposition of $\text{hcf}(m, n)$ and $\text{lcm}(m, n)$.
- (b) Write down, in terms of primes p, q , etc., the prime decompositions of all natural numbers that have eight factors (counting as factors the integer itself and 1). Hence find all natural numbers less than 100 that have eight factors.
- (c) A natural number n is said to be a *practical number* if every natural number r in the range $1 \leq r \leq n$ can be written as a sum of one or more distinct positive factors of n .
- (i) Which of the following are practical?
6, 10, 12, 14, 16
- (ii) Prove that, for each integer $n \geq 1$, the number 2^n is a practical number.

In future we may not be so particular about including the phrase ‘one or more’ and will automatically allow the possibility that a sum contains only one number.

3 The infinitude of the primes

This section explores some properties of the primes, particularly relating to their behaviour as the numbers get bigger.

3.1 Euclid’s Theorem

In Book IX of *Elements*, Euclid produced a simple but elegant proof of the existence of infinitely many primes. The essence of Euclid’s proof comes from consideration of the sequence of numbers $\{P_n\}$, $n \geq 1$, where P_n is obtained by adding 1 to the product of the first n primes:

$$P_1 = 2 + 1 = 3$$

$$P_2 = 2 \times 3 + 1 = 7$$

$$P_3 = 2 \times 3 \times 5 + 1 = 31$$

$$P_4 = 2 \times 3 \times 5 \times 7 + 1 = 211$$

$$P_5 = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$$

$$\vdots$$

It is interesting to note that the first five numbers in this sequence are prime. However, at this point the coincidence ceases as the next number $P_6 = 30\,031 = 59 \times 509$ is composite, as also are P_7 , P_8 , P_9 and P_{10} . The next number P_{11} is prime, but then all the subsequent P_n are composite until P_{75} . At the time of writing this chapter it is not known whether infinitely many numbers in the sequence $\{P_n\}$ are prime, nor indeed

$$P_{75} = 2 \times 3 \times 5 \times \cdots \times 379 + 1.$$

whether infinitely many numbers in this sequence are composite, though at least one of these must be true!

The crucial point concerning the numbers in this sequence is illustrated as follows for the particular term

$$P_5 = 2 \times 3 \times 5 \times 7 \times 11 + 1.$$

Now P_5 is of the form $2r + 1$ and so it has remainder 1 on dividing by 2. Similarly P_5 is of the form $3s + 1$ and so has remainder 1 on dividing by 3. In just the same way P_5 has remainder 1 on dividing by each of the primes 5, 7 and 11. In summary, P_5 has been constructed so that it is not divisible by any of the first five primes, 2, 3, 5, 7 or 11. Now we know, by Proposition 1.2, that P_5 is divisible by some prime and so P_5 ‘uncovers’ a sixth prime; either P_5 is itself prime, or it is divisible by a prime that is not one of the primes 2, 3, 5, 7 or 11 from which it has been constructed.

The same argument applies to each of the numbers

$$P_n = p_1 p_2 p_3 \cdots p_n + 1$$

as follows: P_n is not divisible by any of the primes $p_1, p_2, p_3, \dots, p_n$ as it has remainder 1 on dividing by each of them. So P_n is divisible by some ‘new’ prime.

It follows that there cannot be just a finite number of primes because from such a finite list we can always construct one more.

Let us present this argument formally.

Theorem 3.1 Euclid's Theorem

There are infinitely many primes.

Proof The proof is by contradiction.

Suppose the theorem is not true and that there are only finitely many primes, $p_1, p_2, p_3, \dots, p_n$. Consider the number

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Since N is divisible by some prime, and $p_1, p_2, p_3, \dots, p_n$ are presumed to be the only primes, N is divisible by one of the primes p_i in this list. But then, as p_i divides N and p_i divides $p_1 p_2 \cdots p_i \cdots p_n$, we have that p_i divides the integer combination $N - p_1 p_2 \cdots p_i \cdots p_n$; that is, p_i divides 1. As $p_i \geq 2$ this is a contradiction.

Therefore the supposition that there are only finitely many primes must be false and hence there are infinitely many primes. ■

Euclid's argument can be applied to give an upper bound on the size of the n th prime. Adopting the notation that p_n is the n th prime number, we see that

$$p_{n+1} \leq p_1 p_2 p_3 \cdots p_n + 1$$

and so

$$p_{n+1} < p_n^n + 1.$$

This, however, is not a very useful bound because, for instance, taking $n = 7$ it tells us only that the 8th prime, namely 19, does not exceed $17^7 + 1 \simeq 4.1 \times 10^8$.

Worked Exercise 3.2 finds an alternative upper bound.

Worked Exercise 3.2

Show that the n th prime p_n satisfies the inequality $p_n \leq 2^{2^{n-1}}$.

Solution

Heading towards a proof by the Second Principle of Mathematical Induction, let the statement to be proved be $P(n)$.

The result is true for $n = 1$, since $P(1)$ states that $2 \leq 2^{2^0} = 2$. This gives the basis for the induction.

We now assume that, for some integer $k \geq 1$, $P(1), P(2), \dots, P(k)$ are all true. To complete the induction step we must show that $P(k+1)$ is true; that is, $p_{k+1} \leq 2^{2^k}$.

$$\begin{aligned} p_{k+1} &\leq p_1 p_2 p_3 \cdots p_k + 1, \text{ by Euclid's argument,} \\ &\leq 2 \times 2^2 \times 2^{2^2} \times \cdots \times 2^{2^{k-1}} + 1, \text{ by the induction hypothesis,} \\ &= 2^{1+2+2^2+\cdots+2^{k-1}} + 1, \text{ by the law of indices,} \\ &= 2^{2^k-1} + 1, \text{ by the sum of a geometric progression,} \\ &\leq 2^{2^k-1} + 2^{2^k-1} = 2^{2^k}, \text{ since } 1 \leq 2^{2^k-1} \text{ for all } k. \end{aligned}$$

Hence $P(k+1)$ is true and, by the Second Principle of Mathematical Induction, it follows that $P(n)$ is true for all $n \geq 1$.

The upper bound for the n th prime given in Worked Exercise 3.2 is actually even more extravagant than our previous one. It tells us that the 8th prime now does not exceed $2^{2^7} = 2^{128} \simeq 3.4 \times 10^{38}$. You will be pleased to hear that much better bounds are known.

In 1841, the French mathematician Bertrand (1822–1900) posed an interesting conjecture concerning the location of primes.

Bertrand's Conjecture

For each integer $n \geq 2$, there exists a prime p such that $n < p < 2n$.

Bertrand checked his conjecture for all n up to three million, which, though not quite the daunting task it might at first sound, was nevertheless quite an achievement at that time.

The proof of Bertrand's Conjecture is outside the scope of this module.

A proof was given nine years later, in 1850, by the Russian mathematician Chebyshev (1821–1894). In fact Chebyshev improved on Bertrand’s result by showing that, except for a finite number of values of n , there is always a prime between n and $\frac{6}{5}n$. Yet there is nothing special about Chebyshev’s multiplier $\frac{6}{5}$. It is now known that, for any positive number ε , from any integer n bigger than some number N there is always a prime number between n and $(1 + \varepsilon)n$. As you would expect, the smaller the ε is, the larger the N becomes.

Exercise 3.1

Assuming Bertrand’s Conjecture, prove that the n th prime p_n satisfies the inequality $p_n < 2^n$, for all integers $n \geq 2$.

3.2 Primes in arithmetic progression

Having seen that there are infinitely many primes, it is natural to ask how these primes are distributed amongst the set of integers. As you will discover, interesting questions in this area are plentiful, but answers to them are not so readily at hand. One area in which we can provide some answers concerns the occurrences of primes in arithmetic progressions. For instance, consider the progression

$$3, 7, 11, 15, 19, \dots, 4k + 3, \dots$$

We see that both primes and composites are occurring, and we can ask whether infinitely many members of the sequence are prime. With an eye on Euclid’s proof above we can, with a little care, produce an argument on the same lines to prove that infinitely many of these numbers are prime.

Consider the following sequence of numbers.

$$\begin{aligned} Q_1 &= 4 \times (3) - 1 = 11 \\ Q_2 &= 4 \times (3 \times 7) - 1 = 83 \\ Q_3 &= 4 \times (3 \times 7 \times 11) - 1 = 923 \\ Q_4 &= 4 \times (3 \times 7 \times 11 \times 19) - 1 = 17\,555 \\ &\vdots \end{aligned}$$

In general, the number Q_n is obtained by multiplying together the first n primes in the arithmetic progression (note that composites such as 15 are excluded), then multiplying by 4 and finally subtracting 1. The reason for multiplying by 4 and subtracting 1 is to ensure that Q_n is itself of the form $4k + 3$. The interesting outcome of this is that Q_n turns out to be divisible by a prime of type $4k + 3$ that is larger than any of the n primes involved in its construction. Of the listed values, 11 and 83 are primes of the form $4k + 3$ while

$$923 = 13 \times 71,$$

Note that any number of the form $4q - 1$ is also of the form $4k + 3$ since $4q - 1 = 4(q - 1) + 3$.

where 71 is a prime of the form $4k + 3$, and

$$17\,555 = 5 \times 3511,$$

where 3511 is a prime of the form $4k + 3$. If we can prove that this is generally the case then we are home. We will be able to construct from any n primes in the arithmetic progression a larger prime that is also in the progression, and Euclid's argument by contradiction will be available to us.

But first we digress to present separately a subsidiary result needed in the proof.

Lemma 3.3

Any integer of the form $4k + 3$ is divisible by a prime of this same form.

Proof The Division Algorithm tells us that any integer is of one of the four forms $4q$, $4q + 1$, $4q + 2$ or $4q + 3$. Of these, $4q$ and $4q + 2$ are even and so, with the exception of the prime 2, any number of either of these forms is composite. As $4k + 3$ is not divisible by 2, it follows that it is either prime or is a product of two or more primes each of which is of one of the forms $4q + 1$ or $4q + 3$.

The identity

$$(4m + 1)(4n + 1) = 4(4mn + m + n) + 1$$

shows that the product of any two numbers of the form $4q + 1$ is itself of the form $4q + 1$. It follows that any product of numbers of the form $4q + 1$ is still of the form $4q + 1$. Hence, if $4k + 3$ were divisible only by primes of the form $4q + 1$ it would, itself, be of the form $4q + 1$, which is not the case. Therefore $4k + 3$ must have a prime factor of the form $4q + 3$. ■

Although Lemma 3.3 concerned numbers of the form $4k + 3$, the strategy of the proof can be applied to numbers in some other arithmetic progressions.

Exercise 3.2

Show that any prime $p > 3$ must be of one of the forms $6q + 1$ or $6q + 5$, and hence prove that any number of the form $6k + 5$ must have a prime factor of this same form.

We now complete the proof to which we have been heading.

Theorem 3.4 *Primes of the form $4k + 3$*

There are infinitely many primes of the form $4k + 3$, where k is an integer.

Proof Suppose, to the contrary, that there are only finitely many primes of the form $4k + 3$, say $p_1, p_2, p_3, \dots, p_n$. Consider the integer

$$N = 4(p_1 p_2 p_3 \cdots p_n) - 1 = 4(p_1 p_2 p_3 \cdots p_n - 1) + 3.$$

We observe that N is of the form $4k + 3$, and so, by Lemma 3.3, there is a prime p of form $4k + 3$ that divides N . As $p_1, p_2, p_3, \dots, p_n$ are presumed to be the only primes of the form $4k + 3$, the prime p must be one of this list, say $p = p_i$. But then p divides N and p divides $4(p_1 p_2 p_3 \cdots p_n)$ and so p divides the integer combination $4(p_1 p_2 p_3 \cdots p_n) - N = 1$. That is, p divides 1, which is a contradiction.

Hence there are infinitely many primes of the form $4k + 3$. ■

With the exception of the number 2, all primes are odd. In turn the odd primes fall into two categories, namely those of the form $4k + 1$ and those of the form $4k + 3$. Below we have begun a characterisation of the odd integers from 3 onwards.

prime $4k + 1$	5	13	17	29	37	41	...				
composite	9	15	21	25	27	33	35	39	45	49	...
prime $4k + 3$	3	7	11	19	23	31	43	47	...		

Theorem 3.4 shows that there are infinitely many members in the bottom row. In addition there are certainly infinitely many composites, since any odd multiple of 3, except 3 itself, is an odd composite number. It seems inevitable, therefore, that we should enquire about the top row. Are there infinitely many primes of the form $4k + 1$?

Furthermore, pursuing the infinitely many primes of the form $4k + 3$, these can be split into two categories, namely those of the form $8m + 3$ and those of the form $8m + 7$.

prime $8m + 3$	3	11	19	43	59	67	...
prime $8m + 7$	7	23	31	47	71	79	...

At least one of these lists must be infinite. Are there infinitely many primes of the form $8m + 3$? Are there infinitely many primes of the form $8m + 7$?

All three questions posed above have affirmative answers. However, their proofs are not as elementary as the proof that there are infinitely many primes of the form $4k + 3$ and so we postpone these proofs until we have more mathematical tools at our disposal. Nevertheless, there are other arithmetic progressions for which the question of the infinitude of primes can easily be resolved.

Exercise 3.3

Making use of the result of Exercise 3.2, modify the proof of Theorem 3.4 to prove that there are infinitely many primes of the form $6k + 5$.

All these observations suggest a general question concerning primes in arithmetic progressions. Given *any* two natural numbers a and b are there infinitely many primes of the form $ak + b$, where k is a non-negative integer?

Clearly the answer to this is no. Any common factor of a and b divides each of the integer combinations $ak + b$, and so to have a chance of generating primes we must add the stipulation that $\text{hcf}(a, b) = 1$. Many of the great names of mathematics are associated with assaults on this problem, including Euler (1707–1783). Euler conjectured, but could not prove, that there are infinitely many primes of the form $ak + 1$ for each positive integer a . The ultimate credit for solving this problem goes to Dirichlet (1805–1859), a student of Gauss (1777–1855), who in 1837 used methods of mathematical analysis to prove the result that bears his name.

Euler is pronounced *oiler*.

Theorem 3.5 *Dirichlet's Theorem*

If a and b are positive integers with $\text{hcf}(a, b) = 1$, then there are infinitely many primes of the form $ak + b$, where k is a non-negative integer.

The proof of Dirichlet's Theorem is well beyond the scope of this module.

Before leaving arithmetic progressions, we make the observation that the number of consecutive primes in any such progression is limited. To justify this remark, consider the progression

$$a, a + b, a + 2b, a + 3b, \dots,$$

and suppose that some term $a + rb$ is a prime, say p . Then every p th term thereafter is a multiple of p .

$$\begin{aligned} a + rb &= p \\ a + (r + p)b &= p + pb = p(1 + b) \\ a + (r + 2p)b &= p + 2pb = p(1 + 2b) \\ a + (r + 3p)b &= p + 3pb = p(1 + 3b) \\ &\vdots \\ a + (r + np)b &= p + npb = p(1 + nb) \end{aligned}$$

To illustrate what this argument says, consider the arithmetic progression of numbers of the form $4k + 1$, for $k \in \mathbb{N}$. The first number is 5, which is prime. The argument tells us that every fifth term thereafter, that is, the 6th, 11th, 16th and so on, is divisible by 5, and so is composite. It follows that this sequence cannot have more than five consecutive members all of which are prime.

$a = 7, b = 30$

$a = 7, b = 150$

The numbers

7, 37, 67, 97, 127 and 157

form a sequence of six primes in arithmetic progression, while the numbers

7, 157, 307, 457, 607, 757 and 907

form a sequence of seven primes in arithmetic progression. It is not possible to obtain a sequence of more than seven primes in which the first term is 7, since the eighth term would be divisible by 7.

One can also turn this question around: can we find arbitrarily long arithmetic progressions amongst the primes? The answer to this, discovered in 2004, turns out to be yes: given any k , there exist integers a and b so that

$$a, a + b, a + 2b, \dots, a + (k - 1)b$$

are all prime numbers. This result is known as the Green–Tao Theorem, after its discoverers Ben Green (1977–) and Terence Tao (1975–). However, it is only an *existence* result, in that it does not give any indication of how to find such a sequence. By 2014, the longest sequence that had been found contained only 26 primes.

3.3 Primes generated by polynomials

Whenever n is a multiple of b , $an + b$ is divisible by b and so, if $b \geq 2$, $an + b$ takes infinitely many composite values.

In looking at arithmetic progressions we are really looking at linear functions $f(n) = an + b$, where a and b are positive integers and the domain of f is the non-negative integers. We have seen that some such functions take infinitely many composite values, while others take infinitely many prime values. One question we might pose is whether we can find a simple function that takes only prime values, thereby generating some, or perhaps all, prime numbers. Since we know that such a function cannot be a linear function, the next obvious candidates to try are the quadratic functions.

Table 3.1 lists values of the quadratic $n^2 + n + r$ for some odd integer values of r .

Table 3.1 Values of $n^2 + n + r$, for $r = 1, 7, 11$ and 17 and for $n = 0$ to 12

n	$n^2 + n + 1$	$n^2 + n + 7$	$n^2 + n + 11$	$n^2 + n + 17$
0	1	7	11	17
1	3	$9 = 3^2$	13	19
2	7	13	17	23
3	13	19	23	29
4	$21 = 3 \times 7$	$27 = 3^3$	31	37
5	31	37	41	47
6	43	$49 = 7^2$	53	59
7	$57 = 3 \times 19$	$63 = 3^2 \times 7$	67	73
8	73	79	83	89
9	$91 = 7 \times 13$	97	101	107
10	$111 = 3 \times 37$	$117 = 3^2 \times 13$	$121 = 11^2$	127
11	$133 = 7 \times 19$	139	$143 = 11 \times 13$	149
12	157	163	167	173

Primes appear to crop up quite frequently. In particular, all the listed values for $n^2 + n + 17$ are prime (as would be the values for $n = 13, 14$ and 15 , had we listed them). However, at $n = 16$ this quadratic at last takes a composite value, as $16^2 + 16 + 17 = 289 = 17^2$.

Even more interesting is the quadratic $f(n) = n^2 + n + 41$, the first 40 values of which all turn out to be prime – as shown in Table 3.2.

Table 3.2 $n^2 + n + 41$ is prime for $n = 0, 1, 2, \dots, 39$

n	$f(n)$	n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	10	151	20	461	30	971
1	43	11	173	21	503	31	1033
2	47	12	197	22	547	32	1097
3	53	13	223	23	593	33	1163
4	61	14	251	24	641	34	1231
5	71	15	281	25	691	35	1301
6	83	16	313	26	743	36	1373
7	97	17	347	27	797	37	1447
8	113	18	383	28	853	38	1523
9	131	19	421	29	911	39	1601

In the Middle Ages it was widely believed that all the values taken by this quadratic were prime. However, the next two numbers corresponding to $n = 40$ and $n = 41$ provide counter-examples.

$$f(40) = 40^2 + 40 + 41 = 41^2$$

$$f(41) = 41^2 + 41 + 41 = 41 \times 43$$

In fact, if $f(n) = n^2 + n + r$, then $f(r - 1) = r^2$ is always composite for $r > 1$.

There is another, somewhat curious way in which the numbers arising from this quadratic can be viewed. Suppose that starting at 41, we write down the integers 41, 42, 43, ... in an anticlockwise spiral, as indicated in Figure 3.1.

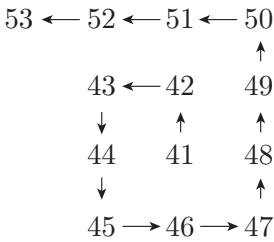


Figure 3.1 Spiralling around 41

Now we remove all the composites, leaving just primes behind, as shown in Figure 3.2.

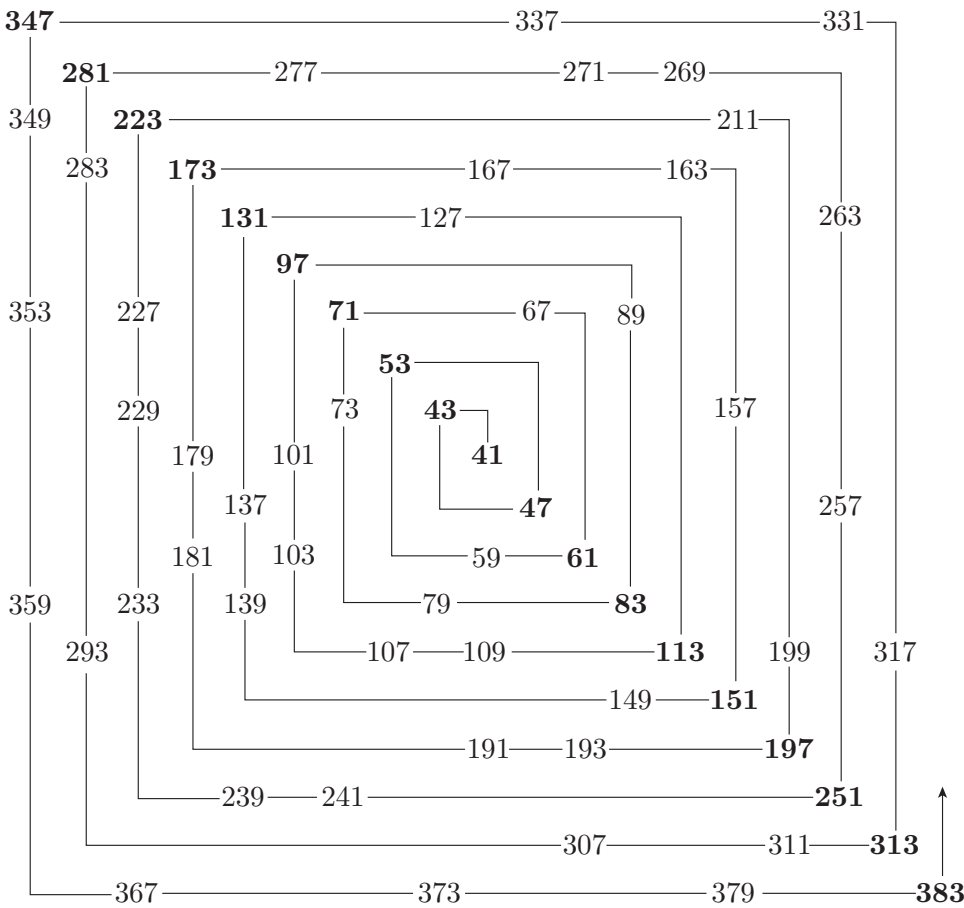


Figure 3.2 The primes from 41 to 383 in spiral formation

It appears that none of the terms on the diagonal from top left to bottom right is removed, and so is prime. The terms on the diagonal are in fact the values of $f(n) = n^2 + n + 41$ for $n \geq 0$. We leave you to convince yourself of this statement.

It turns out that in the values of $n^2 + n + 41$ for $n = 0, 1, 2, \dots, 100$ there are just 14 composite values and 87 primes. Nevertheless, to this day, it is not known whether this quadratic takes infinitely many prime values. (Indeed, the same question has not yet been answered for the simpler quadratic $n^2 + 1$. Are there infinitely many primes that are 1 more than a square?) But we can say some things about factors of $n^2 + n + 41$, as the next worked exercise shows.

Worked Exercise 3.6

Show that:

- (a) $f(n) = n^2 + n + 41$ does not have a prime factor less than 41, for any value of n
- (b) if $f(n)$ is composite, it has a prime factor that is less than or equal to $n + 1$.

Solution

Table 3.2 together with $f(40) = 41^2$ and $f(41) = 41 \times 43$ confirm both claims for integers up to 41, and so we need to consider only integers $n > 41$.

- (a) Aiming for a contradiction to the first claim, suppose that d divides $f(n)$, where $1 < d < 41$. By the Division Algorithm $n = qd + r$, where $0 \leq r < d$. Therefore

$$\begin{aligned} f(n) &= (qd + r)^2 + (qd + r) + 41 \\ &= r^2 + r + 41 + q^2d^2 + 2dqr + qd \\ &= f(r) + d(q^2d + 2qr + q). \end{aligned}$$

Since d divides $f(n)$ and d divides the second term on the right-hand side of this equation, it follows that d divides $f(r)$. But that is a contradiction since, with r lying between 0 and 40, $f(r)$ is known to have no prime factor less than 41.

- (b) For the second claim we simply observe that for $n > 41$,

$$f(n) = n^2 + n + 41 < n^2 + 2n < n^2 + 2n + 1 = (n + 1)^2.$$

Thus if $f(n)$ is composite, then Proposition 1.3 ensures the existence of a prime factor of $f(n)$ that is less than $n + 1$.

Although we are unable to answer the question of whether or not the quadratic function of Worked Exercise 3.6 has infinitely many prime values, we can confirm that it takes infinitely many composite values. In fact it is not difficult to show, appealing to standard properties of

The **degree** of a polynomial $f(n)$ is the highest power of n that occurs in $f(n)$. Polynomials of degree 0 are constant polynomials, which take just the one particular value.

polynomials, that every integer polynomial of degree 1 or more takes infinitely many different composite values.

Exercise 3.4

- (a) Suppose that there are only finitely many primes, say $p_1, p_2, p_3, \dots, p_n$. Show that the number $p_1 + p_2 p_3 \cdots p_n$ is not divisible by any prime in the given list. What can you deduce from this observation?
- (b) Prove that if three prime numbers, all greater than 3, form an arithmetic progression then the common difference of the progression is a multiple of 6. What can you say about the common difference in an arithmetic progression of five primes?
- (c) Consider the sequence of integers $\{n^2 + 3\}$, $n \geq 1$:

4, 7, 12, 19, 28, 39, 52, 67, 84, ...

Prove that consecutive terms of this sequence are either coprime or have a highest common factor of 13.

4 Famous problems concerning primes

The prime numbers have been a notorious source of conjectures and open problems that have eluded resolution. This section explores some of these.

4.1 Proximity of primes

Ignoring the first two primes, 2 and 3, the smallest possible difference between two primes is 2, occurring when two consecutive odd numbers are both prime. Such pairs of primes are called **twin primes**:

3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43;

The *Twin Prime Conjecture* claims that there are infinitely many pairs of twin primes, and remains a famous open problem. There is now substantial numerical evidence, gathered by computer, to support this conjecture (see Table 4.1). A recent breakthrough was made by Yitang Zhang, who in April 2013 proved that there are infinitely many pairs of consecutive primes that differ by no more than some integer n , where n is at most 70 million; the case $n = 2$ would of course resolve the Twin Prime Conjecture. Following the announcement of Zhang's result, an online collaborative project was set up to reduce the bound on n . At the time of writing, the current state-of-the-art is $n \leq 246$, with improvements being made every day.

Table 4.1 Twin primes

n	n th pair of twin primes
1000	79 559, 79 561
2000	182 027, 182 029
3000	300 497, 300 499
4000	424 769, 424 771
5000	557 519, 557 521
6000	690 887, 690 889
7000	833 099, 833 101
8000	974 537, 974 539
9000	1 115 417, 1 115 419
10 000	1 260 989, 1 260 991

Despite the frequency with which successive primes are as close together as possible, it is nevertheless the case that the gap between successive primes can be arbitrarily large, by which we mean that for any given natural number n , no matter how large, there exist n consecutive integers all of which are composite. This is easily demonstrated. Consider the n consecutive integers

$$(n+1)! + 2, (n+1)! + 3, (n+1)! + 4, \dots, (n+1)! + (n+1),$$

where, as usual, $(n+1)! = (n+1) \times n \times \dots \times 3 \times 2 \times 1$. The first of the listed numbers is divisible by 2, the second by 3, the third by 4, and so on, the last being divisible by $n+1$. So these n consecutive integers are all composite.

The same argument shows that the n consecutive numbers

$$(n+1)! - (n+1), (n+1)! - n, \dots, (n+1)! - 3, (n+1)! - 2$$

are composite. So, for each natural number n , of the $2n+3$ numbers consisting of $(n+1)!$ and the symmetrically surrounding numbers, namely

$$\begin{aligned} &(n+1)! - (n+1), (n+1)! - n, \\ &\dots, (n+1)! - 2, (n+1)! - 1, (n+1)!, (n+1)! + 1, (n+1)! + 2, \\ &\dots, (n+1)! + n, (n+1)! + (n+1), \end{aligned}$$

all are composite with the possible exceptions of $(n+1)! - 1$ and $(n+1)! + 1$. This shows that there are long sequences of composite numbers either side of a factorial. If, as illustrated for the case $n=4$ below, both of the numbers $(n+1)! - 1$ and $(n+1)! + 1$ are composite then there will be even longer sequences of composites.

For $n=4$, for which $(n+1)! = 120$, of the eleven numbers

$$115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125,$$

only the two either side of 120 can be prime. As it happens $119 = 7 \times 17$ and $121 = 11^2$, so all 11 are composite. Indeed, we can tack 114 on the beginning and 126 on the end to obtain a sequence of 13 consecutive composite numbers.

A table of primes is given in the Appendix to this chapter.

Exercise 4.1

What is the longest sequence of consecutive composite numbers that includes the number $6! = 720$?

The above considerations suggest that we might look with interest at the sequence of numbers $\{n! + 1\}$, $n = 1, 2, 3, \dots$. Is $n! + 1$ prime for infinitely many n ? This is yet another unsolved problem, although in Chapter 4 we prove a famous result that shows that $n! + 1$ is composite infinitely often.

Moving on from pairs of primes, the next question to ask concerns whether it is possible for three consecutive odd integers to all be prime. Certainly $\{3, 5, 7\}$ is one such set of primes. But this is the only example because, of three consecutive odd integers, one of them must be divisible by 3. We ask you to establish this in the next exercise.

Exercise 4.2

Suppose that n , $n + 2$ and $n + 4$ are three consecutive odd integers. Use the fact that n must be of one of the forms $3k$, $3k + 1$ or $3k + 2$ to show that one of n , $n + 2$ or $n + 4$ is divisible by 3.

The best that we can do with three primes is to find instances of four consecutive odd numbers three of which are prime, such as

5, 7, 11; 7, 11, 13; 11, 13, 17; 13, 17, 19; 17, 19, 23; 37, 41, 43; $\dots$

Such trios of primes are called **prime triplets**. Note that each prime triplet contains a pair of twin primes.

Moving on one stage, we can have two pairs of twin primes with just one missing odd number between them, so that of five consecutive odd numbers four are prime:

5, 7, 11, 13; 11, 13, 17, 19; 101, 103, 107, 109; 191, 193, 197, 199; $\dots$

These are examples of **prime quartets**. Prime quartets are, of course, relatively rare in comparison to twin primes and yet numerical evidence leads to a belief that, still, there are infinitely many prime quartets.

Amongst the integers up to one million there are 166 sets of prime quartets.

4.2 The Goldbach Conjecture

We now consider a problem that is arguably the most famous unsolved problem concerning primes: the so-called Goldbach Conjecture. Its fascination stems from the fact that numerical evidence suggests that it is true, and yet no one has managed to prove it to this day.

The Goldbach Conjecture

Every even integer from 6 onwards can be written as a sum of two odd primes.

The first ten even integers from 6 onwards are expressed as a sum of two odd primes as follows.

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7 = 5 + 5$$

$$12 = 5 + 7$$

$$14 = 3 + 11 = 7 + 7$$

$$16 = 3 + 13 = 5 + 11$$

$$18 = 5 + 13 = 7 + 11$$

$$20 = 3 + 17 = 7 + 13$$

$$22 = 3 + 19 = 5 + 17 = 11 + 11$$

$$24 = 5 + 19 = 7 + 17 = 11 + 13$$

Notice that some of the even integers have several different expressions as the sum of two primes.

Exercise 4.3

Express each of the even numbers from 40 to 60 inclusive as a sum of two odd primes.

By the early twenty-first century, computers had verified the Goldbach Conjecture for even integers up to 10^{17} , but little headway has been made towards a general proof. The most significant development in this direction is a paper by Harald Helfgott (1977–) in April 2013, claiming a proof of the ‘Weak Goldbach Conjecture’, which states that every odd integer is the sum of at most three primes (so that every even integer is the sum of at most four primes). At the time of writing, the proof of this result is still being verified, but it is worth noting that an important component in Helfgott’s proof is a computer search carried out by a former Open University mathematics student!

4.3 The Prime Number Theorem

We have seen plenty of evidence for the unpredictability of occurrences of prime numbers. On the one hand there appear to be infinitely many pairs of consecutive odd integers both of which are prime, whilst at the same time there are arbitrarily long sequences of consecutive integers all of which are composite. But, despite this local irregularity of their

In this module, **log** will always mean the natural logarithm, $\log_e$, sometimes denoted by $\ln$.

distribution, when we look at the primes overall, their global distribution can be described with rather more success.

Towards the end of the eighteenth century, Gauss observed that near an integer x , the probability that a number is prime is approximately $\frac{1}{\log x}$; to be more precise, in the interval from x to $x + N$ (where N is neither too large nor too small), the number of primes is about $\frac{N}{\log x}$. For example, if $x = 10^7$ and $N = 5000$, then

$$\frac{5000}{\log(10^7)} = \frac{5000}{7 \log 10} \simeq 310.2,$$

and there are actually 305 primes between 10 000 000 and 10 005 000.

This led Gauss, still only 15 years of age, to conjecture a result that has become one of the most notorious results of mathematics. When looking at the density of primes in intervals an important function for consideration is $\pi(x)$, defined for each positive real number x to be the number of primes not exceeding x . So, for example, $\pi(6) = 3$ and $\pi(10\sqrt{2}) = 6$. Gauss observed similarities between $\pi(x)$ and the logarithmic integral

$$\text{Li}(x) = \int_2^x \frac{1}{\log t} dt.$$

Gauss had tables of primes up to three million and he compiled a list of the number of primes occurring in consecutive groups of 1000. Table 4.2 provides much more evidence. In it, $\text{Li}(x)$ has been rounded to the nearest integer.

Table 4.2 Density of primes

x	$\pi(x)$	$\text{Li}(x)$
100	25	30
1000	168	178
10 000	1229	1246
100 000	9592	9630
1 000 000	78 498	78 628
10^7	664 579	664 918
10^8	5 761 455	5 762 209
10^{10}	455 052 511	455 055 615
10^{12}	37 607 912 018	37 607 950 281
10^{14}	3 204 941 750 802	3 204 942 065 692

Our values for $\text{Li}(x)$ were determined using the mathematical software package Maple.

The result that Gauss noticed was eventually proved in 1896, almost 100 years after he first conjectured it.

The Prime Number Theorem

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\text{Li}(x)} = 1$$

The determination of $\pi(x)$ involves finding all the primes less than or equal to x . In contrast, $\text{Li}(x)$ can be calculated even for large x by any of the standard ways of approximating integrals. The Prime Number Theorem confirms what is indicated in the above table, namely, that for large x , $\text{Li}(x)$ is a very good approximation to $\pi(x)$.

Gauss was unable to prove the Prime Number Theorem. It was through the collective genius and hard work of several mathematicians in the nineteenth century, notably Dirichlet, Chebyshev, Riemann (1826–1866), Hadamard (1865–1963) and de la Vallée Poussin (1866–1962), that the theorem was finally proved in 1896 by Hadamard and, independently, by de la Vallée Poussin.

The proofs of the Prime Number Theorem given at that time made extensive use of complex function theory, utilising properties of the so-called Riemann zeta function. But in 1949, a purely algebraic proof, not calling on techniques of complex analysis, was discovered by the Norwegian mathematician Selberg (1917–2007). This proof, however, is extremely complicated and beyond the scope of this, or any other, first course in number theory.

On route to proving the Prime Number Theorem by methods of complex analysis, many other results emerge that are interesting in their own right. Two results merit mention here. Many students of mathematics are surprised on first learning that the harmonic series

$$\sum_{n \geq 1} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots$$

is divergent (the sum is unbounded). So, it must come as a real shock to learn that if all the terms are discarded except those where the denominator is prime, then the resulting series

$$\sum_{p \text{ prime}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p} + \cdots$$

is *still* divergent. And yet, despite the firm belief that there are infinitely many pairs of twin primes, if we discard all the terms of the harmonic series except those where the denominator belongs to a pair of twin primes, then the resulting series

$$\sum_{\substack{p \text{ twin} \\ \text{prime}}} \frac{1}{p} = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{29} + \frac{1}{31} + \cdots$$

converges with sum less than 2.

Exercise 4.4

- (a) Show that the sum of twin primes p and $p + 2$, where $p > 3$, is divisible by 12.
- (b) If $n, n + 2, n + 6$ and $n + 8$ is a prime quartet, where $n > 5$, what is the remainder when n is divided by 15?
- (c) Prove that the Goldbach Conjecture is equivalent to the following statement.

Every integer greater than or equal to 6 is a sum of three primes.

- (d) Prove that every even integer from 40 onwards can be expressed as the sum of two odd composite numbers.

Hint: all the numbers of the form $10k$ can be written as $15 + (10k - 15)$.

5 Fibonacci numbers

This final section uses the Division Algorithm to uncover some remarkable properties of a well-known sequence of integers, the Fibonacci sequence.

5.1 The Fibonacci sequence

We have investigated occurrences of primes in sequences

$$f(1), f(2), f(3), \dots,$$

where f is a polynomial with integer coefficients. A further step along this road is to investigate occurrences of primes in recursive sequences, that is, sequences defined by recurrence relations. We restrict ourselves to considering just the best known of all such sequences, the Fibonacci sequence. This sequence has many interesting properties, which we investigate along with its connections with primes.

In his book *Liber Abaci*, written in 1202, Fibonacci posed the following problem.

A pair of rabbits, one male and one female, are confined to an area. The nature of the rabbits is that they produce, on the last day of each month from the second month onwards, a pair of rabbits which, in turn, reproduce in the same way. Assuming that no rabbits die, how many pairs will there be on the first day of each month?

Figure 5.1 shows how the rabbits will breed for the first six months. The dotted lines indicate the continued existence of a pair of rabbits while the arrowed lines indicate the birth of another pair at the end of that month.

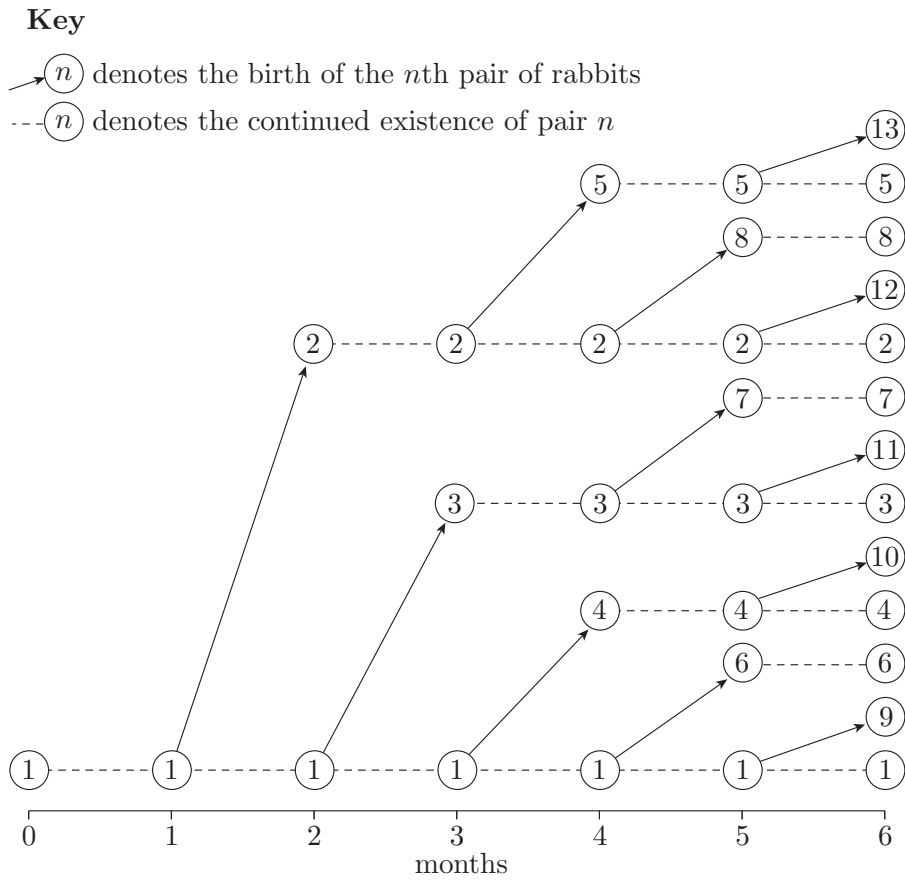


Figure 5.1 Breeding rabbit pairs

If we denote the number of pairs of rabbits alive during month n by F_n , then F_{n+2} is obtained by adding to F_{n+1} the number of births at the end of month $n + 1$. Now there is one birth at the end of month $n + 1$ for each of the F_n pairs alive during month n . Hence the sequence of numbers $\{F_n\}$ is defined by

$$F_1 = F_2 = 1; \text{ and } F_{n+2} = F_{n+1} + F_n, \quad \text{for } n \geq 1.$$

That is, each term, from the third onwards, is the sum of the previous two terms.

The numbers arising in this sequence are called the **Fibonacci numbers**. The first twenty Fibonacci numbers are given in Table 5.1.

Table 5.1 The Fibonacci numbers F_1 to F_{20}

$F_1 = 1$	$F_6 = 8$	$F_{11} = 89$	$F_{16} = 987$
$F_2 = 1$	$F_7 = 13$	$F_{12} = 144$	$F_{17} = 1597$
$F_3 = 2$	$F_8 = 21$	$F_{13} = 233$	$F_{18} = 2584$
$F_4 = 3$	$F_9 = 34$	$F_{14} = 377$	$F_{19} = 4181$
$F_5 = 5$	$F_{10} = 55$	$F_{15} = 610$	$F_{20} = 6765$

On noticing that each of $F_3 = 2$, $F_5 = 5$, $F_7 = 13$ and $F_{11} = 89$ is prime, one is lured towards the conjecture that F_p will be prime whenever p is an odd prime. However, this possibility is shot down just a little further along the sequence:

$$F_{19} = 4181 = 37 \times 113.$$

The occurrences of primes in the Fibonacci sequence pose numerous problems, many of which remain unsolved. In particular, it is believed, but not yet proved, that there are infinitely many prime Fibonacci numbers despite their relative rarity. The first seven *Fibonacci primes* are included in the above list:

$$2, 3, 5, 13, 89, 233 \text{ and } 1597.$$

The next three are

$$F_{23} = 28\,657, F_{29} = 514\,229 \text{ and } F_{43} = 433\,494\,437.$$

On the positive side, it is known that for any prime p , there are infinitely many multiples of p that arise as Fibonacci numbers and that these multiples occur equally spaced in the Fibonacci sequence.

Exercise 5.1

Which of the first twenty Fibonacci numbers are multiples of 3? Is there a pattern to where they occur? Repeat for multiples of 2 and multiples of 5.

The result just cited is not special to primes: for any natural number n , there are infinitely many Fibonacci numbers that are multiples of n and they occur equally spaced in the Fibonacci sequence. We do not prove this result here but, as a lead-in to the topic of congruence, which is the theme of Chapter 3, we illustrate how the result can be demonstrated for a given value of n . We begin with the case $n = 3$ and show that every fourth term in the Fibonacci sequence, and no other, is a multiple of 3.

We start by writing down the sequence obtained from the Fibonacci sequence by replacing each term with its remainder on dividing by 3.

$$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, \dots$$

By the Division Algorithm the terms can only be 0, 1 or 2, where the zeros correspond to the Fibonacci numbers that are divisible by 3. As you can see, so far every fourth term (and no other) is a zero, and what we need to prove is that this pattern continues. The essence of the argument is that we can continue the new (remainder) sequence without reference to the original Fibonacci numbers. As each Fibonacci number is the sum of the previous two, it follows that each term of the remainder sequence is obtained by adding the two previous remainders (and subtracting 3 if necessary). For example, successive terms 2 and 1 in the remainder sequence correspond to Fibonacci numbers of the respective forms $3k + 2$ and $3l + 1$ and the next term,

$$(3k + 2) + (3l + 1) = 3(k + l + 1) + 0,$$

has remainder 0 on division by 3. Our observation merely states that this remainder could have been obtained directly by adding the remainders 2 and 1, and taking the remainder of this resulting sum on dividing by 3. (You will be asked to prove a general result of this type in Exercise 5.2(a).)

The proof is completed by noting that the remainder sequence consists of the pattern 1, 1, 2, 0, 2, 2, 1, 0 recurring indefinitely, since once a pair of consecutive numbers is a repetition of an earlier pair (as will be the pair 1, 1 in this example) the pattern must recur. Hence the zeros in the remainder sequence occur every fourth term and the corresponding Fibonacci numbers are the ones divisible by 3.

This same line of attack can be used to find where the multiples of any integer n occur in the Fibonacci sequence.

Exercise 5.2

- (a) Suppose that the integers a and b have remainders r and s on dividing by the natural number n . Show that $a + b$ and $r + s$ have the same remainder on dividing by n .
- (b) Write out the sequence of remainders obtained when the terms of the Fibonacci sequence are divided by (i) 6 and (ii) 7, and hence find where the multiples of 6 and 7 occur in the Fibonacci sequence.

5.2 Properties of Fibonacci numbers

If it happened that two consecutive Fibonacci numbers were divisible by a common prime p then the sequence of remainders constructed for that prime p would contain consecutive zeros, and hence all terms thereafter would be 0, as can be seen from the fact that if $p \mid F_n$ and $p \mid F_{n+1}$, then $p \mid (F_n + F_{n+1})$, that is, $p \mid F_{n+2}$.

It is clear that this does not happen since to obtain two consecutive zeros, the previous term in the remainder sequence would have had to be 0, as can be seen from the fact that if $p \mid F_n$ and $p \mid F_{n+1}$, then $p \mid (F_{n+1} - F_n)$, that is, $p \mid F_{n-1}$.

Working our way back, the first term would have had to be 0, which it is not. Therefore consecutive Fibonacci numbers are coprime.

There is a nice demonstration of this fact using the Euclidean Algorithm. If we apply the Euclidean Algorithm to find $\text{hcf}(F_{n+1}, F_n)$, the equations involved, except the last, are no more than expressions that each Fibonacci number is the sum of the previous two.

$$\begin{array}{rclcl}
 F_{n+1} & = & 1 \times F_n & + F_{n-1} & 0 < F_{n-1} < F_n \\
 F_n & = & 1 \times F_{n-1} & + F_{n-2} & 0 < F_{n-2} < F_{n-1} \\
 F_{n-1} & = & 1 \times F_{n-2} & + F_{n-3} & 0 < F_{n-3} < F_{n-2} \\
 & \vdots & & & \\
 F_4 & = & 1 \times F_3 & + F_2 & 0 < F_2 < F_3 \\
 F_3 & = & 2 \times F_2 & + 0 &
 \end{array}$$

$F_3 = 2, F_2 = 1.$

The last non-zero remainder is $F_2 = 1$ and so we have proved the following result.

Proposition 5.1 *The coprimality of consecutive Fibonacci numbers*

For any natural number n ,

$$\text{hcf}(F_{n+1}, F_n) = 1.$$

There are many curious identities involving the Fibonacci numbers, a small sample of which is introduced here. Our ambitions in this section are directed towards divisibility properties of Fibonacci numbers. One identity, which will prove to be very useful, is the following.

A useful relationship between Fibonacci numbers

For all integers $m \geq 2$ and $n \geq 1$,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

For instance, putting $m = 7$ and $n = 5$, this identity gives

$$F_{12} = F_{7+5} = F_6F_5 + F_7F_6 = 8 \times 5 + 13 \times 8 = 144,$$

and putting $m = 9$ and $n = 3$,

$$F_{12} = F_{9+3} = F_8F_3 + F_9F_4 = 21 \times 2 + 34 \times 3 = 144.$$

The general identity can be proved using the Second Principle of Mathematical Induction, as we now show.

Worked Exercise 5.2

Prove that for all integers $m \geq 2$ and $n \geq 1$,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

Solution

We prove the result by induction on n . To this end, let $m \geq 2$ be a fixed integer and let $P(n)$ be the proposition that

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

The proposition $P(1)$ states that

$$F_{m+1} = F_{m-1}F_1 + F_mF_2.$$

However, since $F_1 = F_2 = 1$, this is true, being exactly the way that the Fibonacci number F_{m+1} is defined as the sum of its two predecessors. The inductive step requires two previous cases, so to complete the basis for the induction, we also need to verify the proposition $P(2)$:

$$\begin{aligned} F_{m+2} &= F_{m-1}F_2 + F_mF_3 \\ &= F_{m-1} + 2F_m \\ &= F_m + F_{m+1}, \quad \text{since } F_{m+1} = F_{m-1} + F_m. \end{aligned}$$

Hence we have verified the basis for the induction.

We now assume that the proposition $P(n)$ is true for $n = 1, 2, \dots, k$ and proceed to establish its truth when $n = k + 1$. The inductive assumptions, for the cases $n = k - 1$ and $n = k$, are that

$$F_{m+k} = F_{m-1}F_k + F_mF_{k+1}$$

and that

$$F_{m+(k-1)} = F_{m-1}F_{k-1} + F_mF_k.$$

Adding these two, we obtain

$$F_{m+k} + F_{m+(k-1)} = F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k).$$

The sum on the left-hand side of this equation and the two bracketed sums on the right are each the sum of consecutive Fibonacci numbers, and so, by definition,

$$F_{m+(k+1)} = F_{m-1}F_{k+1} + F_mF_{(k+1)+1}.$$

This shows that the proposition $P(k + 1)$ is true as it is the required formula with $n = k + 1$.

Hence, by the Second Principle of Mathematical Induction,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1} \quad \text{for all } m \geq 2 \text{ and } n \geq 1.$$

This argument applies for any $m \geq 2$.

The formula established in Worked Exercise 5.2 helps us to prove the following theorem.

Theorem 5.3 *Divisibility property of the Fibonacci numbers*

For all integers $n > 2$, F_m is divisible by F_n if, and only if, m is divisible by n .

We first remark that the case $n = 2$ has to be excluded because $F_2 = 1$, and so every Fibonacci number is divisible by F_2 , whilst it certainly is not the case that every integer m is divisible by 2.

Proof First we show that if m is a multiple of n , then F_m is a multiple of F_n . To be precise, we show that F_{nq} is a multiple of F_n , for all integers $q \geq 1$, and this we do using mathematical induction.

The result is trivially true when $q = 1$ as it claims that F_n divides F_n . So we have a basis for the induction.

For the induction step, suppose that F_{nq} is divisible by F_n for $q = 1, 2, \dots, k$. We require to prove that $F_{n(k+1)}$ is divisible by F_n . The useful relationship between Fibonacci numbers proved in Worked Exercise 5.2 gives

$$F_{n(k+1)} = F_{nk+n} = F_{nk-1}F_n + F_{nk}F_{n+1}.$$

By the induction hypothesis F_n divides F_{nk} and so F_n divides each of the terms on the right-hand side of this equation. Hence F_n divides $F_{n(k+1)}$, which completes the induction step.

Hence, by the Second Principle of Mathematical Induction, F_{nq} is a multiple of F_n for all integers $q \geq 1$.

It is an ‘if, and only if’ claim, so we require proof in the opposite direction too.

Conversely, we suppose that F_m is divisible by F_n and then have to prove that m is divisible by n . Aiming for a contradiction, suppose $m = nq + r$, where $1 \leq r < n$. Then

$$F_m = F_{nq+r} = F_{nq-1}F_r + F_{nq}F_{r+1}.$$

Now we have just seen, in the first part, that F_{nq} is divisible by F_n and so, as F_m is also divisible by F_n , it follows that F_n divides $F_{nq-1}F_r$. If we can show that $\text{hcf}(F_{nq-1}, F_n) = 1$ the proof will be complete because then Euclid’s Lemma tells us that F_n divides F_r , an obvious contradiction because $F_n > F_r > 0$.

From its construction $\{F_n\}$ is an increasing sequence once $n \geq 2$.

To plug the remaining hole, let $\text{hcf}(F_{nq-1}, F_n) = d$. Then d divides F_n , and so d divides F_{qn} . But then d divides F_{qn-1} and d divides F_{qn} , so d is a common factor of consecutive Fibonacci numbers. Hence, by Proposition 5.1, $d = 1$ as required. ■

We claimed earlier that, for any integer $a \geq 1$, infinitely many multiples of a occur in the Fibonacci sequence with equal spacing. Theorem 5.3 has taken us some distance towards a proof of that result. Suppose that the

first Fibonacci number that is a multiple of a is F_n . Then $F_n, F_{2n}, F_{3n}, \dots$ are equally spaced multiples of a . But are they the only multiples of a ?

Exercise 5.3

Suppose that F_n is the first Fibonacci number that is a multiple of a positive integer a . Show that if F_m is a multiple of a then m is a multiple of n .

Hint: write $m = nq + r$ and use the ‘useful relationship’ as in the proof of Theorem 5.3.

We will leave Fibonacci for now with two final exercises for you.

Exercise 5.4

- (a) It is known that for any prime $p > 5$, either F_{p-1} or F_{p+1} is divisible by p . Confirm that this is true for all primes up to 19.
- (b) Show that $F_n^2 = F_{n+1}F_n - F_nF_{n-1}$ for all integers $n \geq 2$.

Deduce that the sum of the squares of the first n Fibonacci numbers satisfies

$$F_1^2 + F_2^2 + F_3^2 + \dots + F_n^2 = F_{n+1}F_n.$$

Exercise 5.5

- (a) Use the ‘useful relationship between Fibonacci numbers’ to determine F_{22} , F_{23} and F_{24} from the values $F_{10} = 55$, $F_{11} = 89$ and $F_{12} = 144$. Confirm that F_{11} divides F_{22} and that each of F_4 , F_6 , F_8 and F_{12} divides F_{24} .
- (b) (i) Which Fibonacci numbers are multiples of 13?
(ii) Show that 4 divides F_n if, and only if, 8 divides F_n .
- (c) Prove the following identities concerning sums of Fibonacci numbers.
 - (i) $F_1 + F_2 + F_3 + \dots + F_n = F_{n+2} - 1$
 - (ii) $F_1 + F_3 + F_5 + \dots + F_{2n-1} = F_{2n}$
 - (iii) $F_2 + F_4 + F_6 + \dots + F_{2n} = F_{2n+1} - 1$
- (d) (i) Prove that if 2 divides F_n then 4 divides $F_{n+1}^2 - F_{n-1}^2$.
(ii) Prove that if 3 divides F_n then 9 divides $F_{n+1}^3 - F_{n-1}^3$.
- (e) Prove that every natural number can be written as a sum of one or more *distinct* Fibonacci numbers.

Hint: use induction on the claim that, for $n \geq 3$, each integer up to $F_n - 1$ can be written as a sum of one or more distinct numbers from the set $\{F_1, F_2, F_3, \dots, F_{n-1}\}$.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should:

- (a) Understand the term ‘prime number’, and be able to recall basic properties of integers relating to prime numbers.
- (b) Be able to find all prime numbers in a given range using the sieve of Eratosthenes.
- (c) Understand the statement and proof of the Fundamental Theorem of Arithmetic.
- (d) Be able to list all factors of an integer given its prime decomposition; relate prime decompositions to highest common factors and least common multiples.
- (e) Know the meaning of $\tau(n)$, and how to compute it.
- (f) Understand Euclid’s proof of the infinitude of primes, and how this can be used to give an upper bound on the size of the n th prime.
- (g) Understand, and be able to adapt to other situations, the techniques in the proof that there are infinitely many primes of the form $4k + 3$.
- (h) Appreciate the statements of famous conjectures such as the Twin Prime Conjecture and the Goldbach Conjecture, and the statement of the Prime Number Theorem.
- (i) Recall properties of the Fibonacci numbers relating to coprimality and divisibility, and be able to use these properties to solve related exercises.

Solutions to exercises

Solution to Exercise 1.1

- (a) As $11^2 > 117$ we need to test each of the given numbers for divisibility only by 2, 3, 5 and 7.
 111 is divisible by 3, and so is composite.
 113 is not divisible by 2, 3, 5 or 7 and so is prime.
 115 is divisible by 5 and so is composite.
 117 is divisible by 3 and so is composite.
- (b) Since $22 < \sqrt{499} < 23$, it suffices to check divisibility by the primes not exceeding 22, that is, by 2, 3, 5, 7, 11, 13, 17 and 19.

Solution to Exercise 1.2

The primes that do not exceed $\sqrt{200}$ are 2, 3, 5, 7, 11 and 13, so we must cross out all the multiples of these primes occurring in the list of 60 numbers from 141 to 200. The first multiple of 2 in this list is 142, so we cross out 142 and every second number. The first multiple of 3 is 141, so we cross this out along with every third number following it. Similarly we cross out 145 and every fifth number, 147 and every seventh number, 143 and every eleventh number, and 143 and every thirteenth number. The numbers that remain not crossed out are the primes:

149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197 and 199.

Solution to Exercise 1.3

$$168 = 2^3 \times 3 \times 7$$

$$226 = 2 \times 113$$

$$36000 = 2^5 \times 3^2 \times 5^3$$

Solution to Exercise 1.4

- (a) On the one hand if each exponent is even, say $k_i = 2l_i$, then

$$n = p_1^{2l_1} p_2^{2l_2} \cdots p_r^{2l_r} = \left(p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} \right)^2$$

is a square.

On the other hand if n is a square, say $n = a^2$, then writing $a = q_1^{m_1} q_2^{m_2} \cdots q_t^{m_t}$ in its prime decomposition and squaring gives

$$n = q_1^{2m_1} q_2^{2m_2} \cdots q_t^{2m_t}.$$

As the q_i are distinct primes and each m_i is positive, this is the unique prime decomposition of n , revealing that each exponent is even.

Note that a simple modification of this argument generalises the result to any power; an integer is an n th power if, and only if, each of its prime exponents is a multiple of n .

- (b) If $n^3 - 1$ is prime then the given identity expresses a prime as a product of two factors. The uniqueness of prime decomposition tells us that this cannot happen unless one of these factors is 1. Now $n > 1$ (since $n^3 - 1$ is prime) and so $n^2 + n + 1 > 3$. The only possibility is that $n - 1 = 1$, giving $n = 2$ and $n^3 - 1 = 7$.

Solution to Exercise 1.5

- (a) As

$$20! = 1 \times 2 \times 3 \times 4 \times \cdots \times 19 \times 20$$

it is divisible by each of the primes from 2 to 19 inclusive, and by no others.

Looking at the terms on the right-hand side, the primes from 11 to 19 occur just once. The prime 7 occurs twice, in the terms 7 and 14. The prime 5 occurs in terms 5, 10, 15 and 20. The prime 3 occurs once in each term 3, 6, 12 and 15 but twice in terms 9 and 18, making eight occurrences in all. Finally, the prime 2 occurs once in terms 2, 6, 10, 14 and 18, twice in terms 4, 12 and 20, three times in term 8 and four times in term 16, making a total of eighteen occurrences. Hence

$$20! = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19.$$

- (b) Since pq divides a^n , we know that p divides a^n and Euclid's Lemma for prime factors gives p divides a . Similarly, q divides a^n and so q divides a . Now as p and q are distinct primes, $\text{hcf}(p, q) = 1$ and so pq divides a ; say $(pq)r = a$. But then, raising to the n th power, $(pq)^n r^n = a^n$, which confirms that $(pq)^n$ divides a^n .
- (c) Suppose that $3p + 1$ is a square, say $3p + 1 = n^2$. Then

$$3p = n^2 - 1 = (n - 1)(n + 1).$$

Now $n > 2$, since $p \geq 2$, and so the right-hand side of this equation is a product of two factors each exceeding 1. The left-hand side is the product of two primes. By uniqueness of prime decomposition we must have either $3 = n - 1$ and $p = n + 1$, or alternatively $3 = n + 1$ and $p = n - 1$. The former case leads to $n = 4$ and $p = 5$, which is one solution. The latter case leads to $n = 2$ and $p = 1$, which is invalid.

- (d) Thinking in terms of remainders on division by 3, there are three possibilities for the prime p : it is 3, of form $3k + 1$, or of form $3k + 2$.

If $p = 3$ then $8p + 1 = 25$ is composite.

If $p = 3k + 1$ then $8p + 1 = 24k + 9 = 3(8k + 3)$ is composite.

If $p = 3k + 2$ then $8p - 1 = 24k + 15 = 3(8k + 5)$ is composite.

- (e) The prime p must take one of the twelve forms $12k + r$, where $0 \leq r \leq 11$. However, when r is even $12k + r$ is divisible by 2, and similarly $12k + r$ is divisible by 3 when $r = 3$ or 9. The only remaining possibilities are $12k + 1$, $12k + 5$, $12k + 7$ and $12k + 11$, and any prime $p \geq 5$ must take one of these forms.

We are told that $p \geq 5$ and so $p = 2$ and $p = 3$ are not possibilities.

Now

$$(12k+1)^2 = 24(6k^2+k) + 1,$$

$$(12k+5)^2 = 24(6k^2+5k+1) + 1,$$

$$(12k+7)^2 = 24(6k^2+7k+2) + 1,$$

$$\text{and } (12k+11)^2 = 24(6k^2+11k+5) + 1.$$

So whichever of the four forms p takes, p^2 is of the form $24m+1$.

If q is another such prime, say $q^2 = 24n+1$, then

$$p^2 - q^2 = (24m+1) - (24n+1) = 24(m-n)$$

which is divisible by 24.

(f) Consider the given factorisation

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + \cdots + a + 1).$$

For $a^n - 1$ to be prime, one of the two factors on the right-hand side of this equation will have to be equal to 1. The only way this can happen is when $a-1=1$, so that $a=2$.

Next, suppose that n is composite, say $n=rs$, where $r>1$ and $s>1$. Then $2^n - 1 = (2^r)^s - 1$, and so replacing a by 2^r and replacing n by s in the above factorisation:

$$(2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + 2^{r(s-3)} + \cdots + 2^r + 1).$$

Once again this expresses $2^n - 1$ as a product of two factors and, this time, since $2^r > 2$ neither factor is equal to 1. This contradicts the primality of $2^n - 1$. The only assumption we have made is that $n=rs$ is composite. Hence we conclude that n must be prime.

Solution to Exercise 2.1

In total, there are 18 factors of 252, including itself and 1, but what you should observe is that the prime decomposition of each factor d involves only the primes 2, 3 and 7. What is more, since 2^3 does not divide 252 the exponent of 2 in the factor d must be less than 3. Similarly the exponent of 3 in d cannot exceed 2 and the exponent of 7 in d cannot exceed 1. The conclusion to be drawn is that the factors of 252 are the integers $2^r \times 3^s \times 7^t$, where $r=0, 1$ or 2 , $s=0, 1$ or 2 and $t=0$ or 1 . The three choices for r , three choices for s and two choices for t give a total of $3 \times 3 \times 2 = 18$ factors, which are distinct due to the uniqueness of prime decomposition.

Solution to Exercise 2.2

(a) The factors of m are the integers $3^r \times 5^s \times 17^t$, where $0 \leq r \leq 3$, $0 \leq s \leq 1$ and $0 \leq t \leq 2$. That makes $4 \times 2 \times 3 = 24$ factors in all.

The same reasoning gives $2 \times 3 \times 2 \times 5 = 60$ factors of n .

(b) The common factors of m and n are

$$1, 3, 3^2, 17, 3 \times 17, 3^2 \times 17, 3 \times 17^2 \text{ and } 3^2 \times 17^2.$$

(c) The answer in part (b) lists all the common factors of m and n , the largest one, $3^2 \times 17^2$, being the required value of $\text{hcf}(m, n)$.

$$\begin{aligned} \text{lcm}(m, n) &= \frac{mn}{\text{hcf}(m, n)} \\ &= \frac{3^3 \times 5 \times 17^2 \times 2 \times 3^2 \times 7 \times 17^4}{3^2 \times 17^2} \\ &= 2 \times 3^3 \times 5 \times 7 \times 17^4, \text{ using Proposition 4.15 of Chapter 1} \end{aligned}$$

Solution to Exercise 2.3

The six primes 2, 3, 5, 7, 11 and 19 are involved in m or n . For the highest common factor we write down the lower exponent (possibly 0) for each prime, while for the least common multiple we write down the larger exponent for each prime:

$$\begin{aligned} \text{hcf}(m, n) &= 2^0 \times 3^2 \times 5^0 \times 7^0 \times 11^1 \times 19^0 = 3^2 \times 11, \\ \text{lcm}(m, n) &= 2 \times 3^3 \times 5^3 \times 7 \times 11 \times 19. \end{aligned}$$

Solution to Exercise 2.4

24 can be expressed as a product of factors in the following ways:

$$24, 2 \times 12, 2 \times 2 \times 6, 2 \times 3 \times 4, 2 \times 2 \times 2 \times 3, 3 \times 8, 4 \times 6.$$

Accordingly, a number with any of the following prime decompositions will have 24 factors:

$$p_1^{23}, p_1 p_2^{11}, p_1 p_2 p_3^5, p_1 p_2^2 p_3^3, p_1 p_2 p_3 p_4^2, p_1^2 p_2^7, p_1^3 p_2^5.$$

The smallest of each type is, respectively,

$$2^{23}, 2^{11} \times 3, 2^5 \times 3 \times 5, 2^3 \times 3^2 \times 5, 2^2 \times 3 \times 5 \times 7, 2^7 \times 3^2, 2^5 \times 3^3.$$

The smallest of these is $2^3 \times 3^2 \times 5 = 360$.

Solution to Exercise 2.5

(a) First we have the factorisation

$$n = 3344 = 2^4 \times 11 \times 19.$$

For each prime that divides either m or n , we take the lesser exponent to get $\text{hcf}(m, n)$ and the greater exponent to get $\text{lcm}(m, n)$. Therefore

$$\text{hcf}(2^3 \times 3^2 \times 7 \times 11, 2^4 \times 11 \times 19) = 2^3 \times 11$$

and

$$\text{lcm}(2^3 \times 3^2 \times 7 \times 11, 2^4 \times 11 \times 19) = 2^4 \times 3^2 \times 7 \times 11 \times 19.$$

(b) The integer 8 can be written as a product of non-trivial factors in three ways, namely $2 \times 2 \times 2$, 2×4 and 8. Accordingly, numbers with each of the following prime decompositions will have exactly eight factors:

$$p \times q \times r, p \times q^3, p^7, \text{ where } p, q \text{ and } r \text{ are any distinct primes.}$$

As $2^7 = 128$, all numbers of form p^7 exceed 100. Those of the other forms that do not exceed 100 are

$$\begin{aligned} 2 \times 3 \times 5 &= 30, & 2 \times 3 \times 7 &= 42, & 2 \times 3 \times 11 &= 66, & 2 \times 3 \times 13 &= 78, \\ 2 \times 5 \times 7 &= 70, & 2^3 \times 3 &= 24, & 2^3 \times 5 &= 40, & 2^3 \times 7 &= 56, \\ 2^3 \times 11 &= 88, & 3^3 \times 2 &= 54. \end{aligned}$$

- (c) (i) The integer 6 is practical. The numbers 1 to 6 respectively are expressed as sums of distinct factors as

$$1, 2, 3, 1 + 3, 2 + 3, 6.$$

10 is not practical. Its factors are 1, 2, 5 and 10, but 4 (and 9) cannot be expressed as a sum of these without repeats.

12 is practical. The numbers 1 to 12 are sums of factors as follows:

$$1, 2, 3, 4, 2 + 3, 6, 1 + 6, 2 + 6, 3 + 6, 4 + 6, 2 + 3 + 6, 12.$$

14 is not practical. For example, 4 cannot be expressed as a sum of numbers from $\{1, 2, 7, 14\}$ with no repeats.

16 is practical. The numbers 1 to 8 are given, respectively, by

$$1, 2, 1 + 2, 4, 1 + 4, 2 + 4, 1 + 2 + 4, 8.$$

The numbers from 9 to 15 are obtained by adding the factor 8 to the first seven of the above expressions. 16 is just itself.

- (ii) The demonstration that 16 is a practical number reveals a pattern that will persist for any power of 2. But to make it ‘watertight’ we appeal to induction.

Let $P(n)$ be the statement that every integer in the range 1 to $2^n - 1$ can be written as a sum of distinct members of the set $\{1, 2, 2^2, 2^3, \dots, 2^{n-1}\}$. (This is equivalent to what is required; we have just excluded the obvious case of 2^n itself being written as the factor 2^n .)

The basis for induction is immediate as $P(1)$ claims no more than that 1 can be written as a sum of members of $\{1\}$.

For the induction step, suppose that $P(k)$ is true and let m be any integer in the range 1 to $2^{k+1} - 1$. If $m < 2^k$ then the induction hypothesis tells us that it is a sum of distinct members of

$$\{1, 2, 2^2, 2^3, \dots, 2^{k-1}\}$$

and there is nothing to prove. On the other hand, if $m \geq 2^k$ then $m - 2^k < 2^k$ and the induction hypothesis tells us that $m - 2^k$ can be written as a sum of distinct members of the set

$$\{1, 2, 2^2, 2^3, \dots, 2^{k-1}\}.$$

Addition of 2^k then gives m written as a sum of distinct members of the set

$$\{1, 2, 2^2, 2^3, \dots, 2^{k-1}, 2^k\},$$

showing the truth of $P(k + 1)$.

Hence, by mathematical induction, $P(n)$ is true for all integers $n \geq 1$.

Solution to Exercise 3.1

Let $P(n)$ be the proposition that the n th prime p_n is less than 2^n .

$P(2)$ is true since the second prime $p_2 = 3$ and $3 < 2^2$, giving the basis for the induction.

Suppose that, for some integer $k \geq 2$, $P(k)$ is true. That is,

$$p_k < 2^k.$$

By Bertrand's Conjecture, there is a prime, say q , lying between 2^k and 2^{k+1} . Putting the two facts together,

$$p_k < 2^k < q < 2^{k+1}.$$

Now, as q is a prime exceeding p_k ,

$$p_{k+1} \leq q,$$

and so

$$p_{k+1} < 2^{k+1},$$

which confirms the truth of $P(k+1)$.

Hence, by mathematical induction, $P(n)$ is true for all integers $n \geq 2$.

Solution to Exercise 3.2

Any integer takes one of the six forms $6q$, $6q+1$, $6q+2$, $6q+3$, $6q+4$ or $6q+5$. Of these, $6q$, $6q+2$ and $6q+4$ are even while $6q+3$ is divisible by 3. Hence, with the exception of primes 2 and 3, any prime is of one of the forms $6q+1$ or $6q+5$.

The identity

$$(6m+1)(6n+1) = 6(6mn+m+n) + 1$$

shows that the product of numbers of the form $6q+1$ is itself of this form. Therefore the number $6k+5$, which is not divisible by either 2 or 3, cannot have all its prime factors of the form $6q+1$ and so must be divisible by a prime of form $6q+5$.

Solution to Exercise 3.3

Suppose to the contrary that there are only finitely many primes of the form $6k+5$, say, $p_1, p_2, p_3, \dots, p_n$, and consider the number

$$N = 6(p_1 p_2 p_3 \cdots p_n) - 1 = 6(p_1 p_2 p_3 \cdots p_n - 1) + 5.$$

We observe that N is of the form $6k+5$, and so by Exercise 3.2 there is a prime p of form $6k+5$ that divides N . As $p_1, p_2, p_3, \dots, p_n$ are presumed to be the only primes of the form $6k+5$, p must be one of this list, say $p = p_i$. But then p is a factor of N and also of $6(p_1 p_2 p_3 \cdots p_n)$ and so p divides $6(p_1 p_2 p_3 \cdots p_n) - N$, that is, p divides 1, giving the required contradiction.

Solution to Exercise 3.4

- (a) Suppose that $p_1, p_2, p_3, \dots, p_n$ are the only primes. Consider $N = p_1 + p_2 p_3 \cdots p_n$. If p_1 divides N , then p_1 divides $N - p_1$. That is, p_1 divides $p_2 p_3 \cdots p_n$. The Corollary to Euclid's Lemma for prime factors now gives $p_1 = p_i$ for some $2 \leq i \leq n$, which is a contradiction.

Similarly, if p_i divides N for some $2 \leq i \leq n$, then p_i divides $(N - p_2 p_3 \cdots p_n)$; that is, p_i divides p_1 , which is impossible.

Hence N is not divisible by any of the primes $p_1, p_2, p_3, \dots, p_n$.

This amounts to an alternative proof of the infinitude of the primes. It shows that there cannot be just n primes because, from such a list of n primes, we can always construct another prime; the number N has to be divisible by some prime but not one of the primes in the 'list'.

- (b) Suppose that $p, p + d$ and $p + 2d$ are three primes, where $p > 3$.

We first note that d must be even because otherwise one of p or $p + d$ would be even, contrary to the fact that they are odd primes.

In a similar way, d must be divisible by 3 because otherwise one of $p + d$ or $p + 2d$ is divisible by 3, contrary to the fact that they are primes. The following table illustrates why this is so. The prime $p > 3$ must be one of the forms $3k + 1$ or $3k + 2$ and each possibility $d = 3r + 1$ or $d = 3r + 2$ leads to either $p + d$ or $p + 2d$ being divisible by 3.

	$d = 3r + 1$	$d = 3r + 2$
$p = 3k + 1$	$p + 2d = 3(k + 2r + 1)$	$p + d = 3(k + r + 1)$
$p = 3k + 2$	$p + d = 3(k + r + 1)$	$p + 2d = 3(k + 2r + 2)$

We conclude that d is divisible by both 2 and 3 and hence by 6.

For five primes in arithmetic progression, $p, p + d, p + 2d, p + 3d$ and $p + 4d$, we have already shown that d is divisible by 6. A repeat of the above argument shows that if d is not a multiple of 5, then one of the five numbers must be divisible by 5. Of course $p = 5$ is now possible, and indeed $p = 5, d = 6$ gives the arithmetic progression 5, 11, 17, 23, 29 of five primes. When $p > 5$ we must have that d is divisible by both 6 and 5 and, as $\text{hcf}(5, 6) = 1$, d is a multiple of 30.

- (c) Successive terms of the given sequence are $n^2 + 3$ and $(n + 1)^2 + 3$. Let d be the highest common factor of these two numbers. Then

$$d \mid ((n + 1)^2 + 3 - (n^2 + 3)); \text{ that is, } d \mid 2n + 1.$$

Therefore

$$d \mid (n(2n + 1) - 2(n^2 + 3)); \text{ that is, } d \mid n - 6.$$

Therefore

$$d \mid (2n + 1 - 2(n - 6)); \text{ that is, } d \mid 13.$$

Hence $\text{hcf}(n^2 + 3, (n + 1)^2 + 3) = 1$ or 13.

We repeatedly use the fact that if d divides two numbers, then it divides any integer combination of them.

Solution to Exercise 4.1

For the case $n = 5$, for which $(n + 1)! = 720$, there are sequences of five consecutive composite numbers either side of 720. To be specific, we know that 714, 715, 716, 717, 718, 720, 722, 723, 724, 725 and 726 are composite. Of the two missing numbers, 719 is prime – you might have tested divisibility by each of the primes from 2 to 23 inclusive, though reference to the table of primes given in the Appendix would have eased your task – and 721 is composite, being divisible by 7. The sequence of seven consecutive composites from 720 to 726 inclusive does not extend because the next higher number, 727, is also prime.

Solution to Exercise 4.2

If $n = 3k$ then n is divisible by 3.

If $n = 3k + 1$ then $n + 2 = 3k + 3$ is divisible by 3.

If $n = 3k + 2$ then $n + 4 = 3k + 6$ is divisible by 3.

Solution to Exercise 4.3

Each of these numbers has three or more ways of being written as a sum of two odd primes. We give just one way for each.

$$\begin{array}{ll} 40 = 3 + 37 & 52 = 5 + 47 \\ 42 = 5 + 37 & 54 = 23 + 31 \\ 44 = 3 + 41 & 56 = 19 + 37 \\ 46 = 23 + 23 & 58 = 17 + 41 \\ 48 = 5 + 43 & 60 = 7 + 53 \\ 50 = 19 + 31 \end{array}$$

Solution to Exercise 4.4

See Exercise 1.5(e) of Section 1.

- (a) Any number is of one of the forms $12k + r$, $0 \leq r \leq 11$. To be a prime (excluding the primes 2 and 3), r must take one of the values 1, 5, 7 or 11. But $p + 2$ is also prime. This eliminates the possibility $r = 1$ for which $p + 2 = 12k + 3$, which is divisible by 3. It also eliminates $r = 7$ which gives $p + 2 = 12k + 9$, again divisible by 3. The remaining possibilities are

$$p = 12k + 5, \quad p + 2 = 12k + 7,$$

giving

$$p + (p + 2) = 24k + 12,$$

and

$$p = 12k + 11, \quad p + 2 = 12k + 13 = 12(k + 1) + 1,$$

giving

$$p + (p + 2) = 24k + 24.$$

In both cases the sum of the twin primes is divisible by 12.

- (b) Consider the five consecutive odd integers $n, n + 2, n + 4, n + 6$ and $n + 8$. One of these numbers is divisible by 5 (see Exercise 3.4(b) of Section 3) and, of any three in succession, one is divisible by 3. So, for $n > 5$, $n, n + 2, n + 6$ and $n + 8$ can all be prime only when $n + 4$ is divisible by both 3 and 5 (and therefore by 15). So $n + 4 = 15k$, giving $n = 15k - 4 = 15(k - 1) + 11$, and the required remainder is 11.
- (c) Suppose that the Goldbach Conjecture holds. Then, for any $n \geq 4$, $2n - 2 \geq 6$ and so can be written as a sum of two odd primes, say $2n - 2 = p_1 + p_2$. Hence

$$2n = p_1 + p_2 + 2 \quad \text{and} \quad 2n + 1 = p_1 + p_2 + 3,$$

showing that $2n$ and $2n + 1$ can be written as the sum of three primes. Therefore all integers from 8 onwards can be written in this form. The two remaining integers, 6 and 7, can also be expressed as a sum of three primes since

$$6 = 2 + 2 + 2 \quad \text{and} \quad 7 = 2 + 2 + 3.$$

Conversely, suppose that every integer greater than or equal to 6 can be written as the sum of three primes and consider the even integer $2n$, for $n \geq 3$.

We know that

$$2n + 2 = p_1 + p_2 + p_3,$$

where p_1, p_2 and p_3 are prime.

But p_1, p_2 and p_3 cannot all be odd for, if so, the sum on the right-hand side is odd. So one of the p_i is 2; say $p_3 = 2$. In this case

$$2n = p_1 + p_2.$$

Finally, if either of p_1 or p_2 is 2 then, as $p_1 + p_2$ is even, so too is the other, contradicting the fact that $n \geq 3$.

Hence $2n$ is expressed as the sum of two odd primes, which is the Goldbach Conjecture.

- (d) The even integers take one of the five forms $10k, 10k + 2, 10k + 4, 10k + 6$ or $10k + 8$. We can write each of these as the sum of two composite numbers as follows:

$$10k = 15 + (10k - 15), \quad k \geq 3;$$

$$10k + 2 = 27 + (10k - 25), \quad k \geq 4;$$

$$10k + 4 = 9 + (10k - 5), \quad k \geq 2;$$

$$10k + 6 = 21 + (10k - 15), \quad k \geq 3;$$

$$10k + 8 = 33 + (10k - 25), \quad k \geq 4.$$

The second term in each sum is divisible by 5 and hence is composite provided it exceeds 5; however, the given condition on k ensures this. Note that 38 is the largest even number that cannot be expressed in this way.

Solution to Exercise 5.1

The multiples of 3 are F_4, F_8, F_{12}, F_{16} and F_{20} . It appears that every fourth term is a multiple of 3. Similarly, every third term – and these alone – appear to be multiples of 2, and every fifth term is a multiple of 5.

Solution to Exercise 5.2

- (a) Let $a = q_1n + r$ and $b = q_2n + s$. Now let t be the remainder when $r + s$ is divided by n ; that is,

$$r + s = q_3n + t, \quad 0 \leq t < n,$$

for some integer q_3 . Adding the first two equations gives

$$\begin{aligned} a + b &= q_1n + q_2n + r + s \\ &= q_1n + q_2n + q_3n + t \\ &= (q_1 + q_2 + q_3)n + t. \end{aligned}$$

Hence, by the uniqueness of remainder, t is also the remainder on dividing $a + b$ by n .

- (b) (i) The remainder sequence on dividing by 6 begins

$$1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, 1, \dots$$

The sequence repeats after 24 terms and the zeros occur at terms 12 and 24. Hence every twelfth term of the Fibonacci sequence is divisible by 6.

- (ii) The remainder sequence on dividing by 7 begins

$$1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, \dots,$$

repeating after 16 terms, so zeros occur every eighth term and these correspond to the Fibonacci numbers that are divisible by 7.

Solution to Exercise 5.3

Suppose that F_n is the first multiple of a in the Fibonacci sequence and that F_m is any other multiple of a . Let $m = nq + r$, where $0 \leq r < n$. Then, if $r \neq 0$ we can apply the ‘useful relationship’ and write

$$F_m = F_{nq+r} = F_{nq-1}F_r + F_{nq}F_{r+1}.$$

Now a divides both F_m and F_{nq} (the latter by Theorem 5.3), and so a divides $F_{nq-1}F_r$.

But from $\text{hcf}(F_{nq-1}, F_{nq}) = 1$, and the fact that a divides F_{nq} , it follows that $\text{hcf}(a, F_{nq-1}) = 1$. Since a divides $F_{nq-1}F_r$, Euclid’s Lemma now gives that a divides F_r .

Finally, as $0 < r < n$ and F_n is the first multiple of a , we have a contradiction. So $r = 0$. Hence $m = nq$ and m is a multiple of n .

Solution to Exercise 5.4

- (a) $F_8 = 21$ is divisible by 7.
 $F_{10} = 55$ is divisible by 11.
 $F_{14} = 377$ is divisible by 13.
 $F_{18} = 2584$ is divisible by both 17 and 19.
- (b) $F_{n+1}F_n - F_nF_{n-1} = F_n(F_{n+1} - F_{n-1}) = F_n^2$, for $n \geq 2$.

Therefore

$$\begin{aligned}
 & F_1^2 + F_2^2 + F_3^2 + F_4^2 + \cdots + F_n^2 \\
 &= F_1^2 + (F_3F_2 - F_2F_1) + (F_4F_3 - F_3F_2) \\
 &\quad + (F_5F_4 - F_4F_3) + \cdots + (F_{n+1}F_n - F_nF_{n-1}) \\
 &= F_1^2 - F_2F_1 + F_{n+1}F_n, \quad \text{all other terms cancelling,} \\
 &= F_{n+1}F_n, \quad \text{since } F_1 = F_2 = 1.
 \end{aligned}$$

This result lends itself to a simple induction proof, but here we were asked to deduce it from the earlier property.

Solution to Exercise 5.5

- (a) $F_{22} = F_{11+11} = F_{10}F_{11} + F_{11}F_{12} = F_{11}(F_{10} + F_{12})$
 $= 89(55 + 144) = 17\,711.$
 $F_{23} = F_{12+11} = F_{11}F_{11} + F_{12}F_{12}$
 $= 89^2 + 144^2 = 28\,657.$
 $F_{24} = F_{22} + F_{23} = 17\,711 + 28\,657 = 46\,368.$
 $F_{22} = 89 \times 199 = F_{11} \times 199.$
 $F_{24} = 46\,368 = F_4 \times 15\,456 = F_6 \times 5796 = F_8 \times 2208 = F_{12} \times 322.$
- (b) (i) $F_7 = 13$ and hence, by Theorem 5.3 and Exercise 5.3, F_n is a multiple of 13 if, and only if, n is a multiple of 7. Therefore, the multiples of 13 occur every seventh term.
- (ii) As $F_6 = 8$ the multiples of 8 occur every sixth term. The first multiple of 4 that is a Fibonacci number is also $F_6 = 8$. So the multiples of 4 also occur every sixth term and are the same as the multiples of 8.
- (c) (i) The identity

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$$

is readily seen by adding the equations in the system

$$F_1 = F_3 - F_2$$

$$F_2 = F_4 - F_3$$

$$F_3 = F_5 - F_4$$

$$\vdots$$

$$F_n = F_{n+2} - F_{n+1}$$

and noting that all the terms on the right cancel except $F_{n+2} - F_2$. The fact that $F_2 = 1$ completes the argument.

A rather more formal proof is given by mathematical induction.

Let $P(n)$ be the claim of the identity.

Putting in values for $n = 1$ we get

$$1 = 2 - 1,$$

which is true, providing the basis for induction.

So suppose $P(k)$ is true, for some $k \geq 1$; that is,

$$F_1 + F_2 + F_3 + \cdots + F_k = F_{k+2} - 1.$$

Adding F_{k+1} to both sides gives

$$\begin{aligned} F_1 + F_2 + F_3 + \cdots + F_k + F_{k+1} &= F_{k+1} + F_{k+2} - 1 \\ &= F_{k+3} - 1, \end{aligned}$$

completing the induction step.

The result follows by mathematical induction.

- (ii) Again, proof by mathematical induction is straightforward. The result is true for $n = 1$ since it asserts that $F_1 = F_2$. The assumption of its truth for $n = k$, namely,

$$F_1 + F_3 + F_5 + \cdots + F_{2k-1} = F_{2k}$$

leads immediately to

$$F_1 + F_3 + F_5 + \cdots + F_{2k-1} + F_{2k+1} = F_{2k} + F_{2k+1} = F_{2k+2},$$

this being the claim for $n = k + 1$, which completes the induction step.

The result follows by mathematical induction.

- (iii) You may have proved this result by mathematical induction. Alternatively, we can make use of the two previous results. Take the two equations

$$\begin{aligned} F_1 + F_2 + F_3 + \cdots + F_{2n} &= F_{2n+2} - 1, \\ F_1 + F_3 + F_5 + \cdots + F_{2n-1} &= F_{2n}, \end{aligned}$$

established in parts (i) and (ii). Subtraction gives

$$\begin{aligned} F_2 + F_4 + F_6 + \cdots + F_{2n} &= F_{2n+2} - F_{2n} - 1 \\ &= F_{2n+1} + F_{2n} - F_{2n} - 1 \\ &= F_{2n+1} - 1. \end{aligned}$$

- (d) (i) Write

$$\begin{aligned} F_{n+1}^2 - F_{n-1}^2 &= (F_{n+1} - F_{n-1})(F_{n+1} + F_{n-1}) \\ &= F_n(F_n + 2F_{n-1}), \quad \text{using } F_{n+1} = F_n + F_{n-1}. \end{aligned}$$

Now if 2 divides F_n then 2 divides $F_n + 2F_{n-1}$, and so 4 divides $F_{n+1}^2 - F_{n-1}^2$.

- (ii) Write

$$\begin{aligned} F_{n+1}^3 - F_{n-1}^3 &= (F_{n+1} - F_{n-1})(F_{n+1}^2 + F_{n+1}F_{n-1} + F_{n-1}^2) \\ &= F_n((F_n + F_{n-1})^2 + (F_n + F_{n-1})F_{n-1} + F_{n-1}^2), \\ &\quad \text{using } F_{n+1} = F_n + F_{n-1}, \\ &= F_n(F_n^2 + 3F_nF_{n-1} + 3F_{n-1}^2). \end{aligned}$$

Now if 3 divides F_n then 3 divides $F_n^2 + 3F_nF_{n-1} + 3F_{n-1}^2$, and so 9 divides $F_{n+1}^3 - F_{n-1}^3$.

- (e) Let $P(n)$ be the claim that, for $n \geq 3$, each integer from 1 up to $F_n - 1$ can be written as a sum of one or more distinct Fibonacci numbers from the set $\{F_1, F_2, \dots, F_{n-1}\}$.

For the case $n = 3$, $F_3 - 1 = 1$ and the only number in the range 1 to $F_3 - 1$ is 1 itself. But $1 = F_1$, providing the basis for induction.

With the Second Principle of Mathematical Induction in mind, suppose that each of $P(3), P(4), \dots, P(k)$ is true and consider $P(k+1)$. Let m be any integer in the range $1 \leq m < F_{k+1}$. If $m < F_k$ then, by $P(k)$, m can be written as a sum of distinct Fibonacci numbers from the set $\{F_1, F_2, \dots, F_{k-1}\}$.

On the other hand, if $m \geq F_k$ then either $m = F_k$, in which case it is a sum of one Fibonacci number, or $m > F_k$. In this latter case

$$m - F_k < F_{k+1} - F_k = F_{k-1}$$

and so, by $P(k-1)$, $m - F_k$ can be written as a sum of distinct Fibonacci numbers from the set $\{F_1, F_2, \dots, F_{k-2}\}$. By adding F_k to both sides, m is then written as a sum of distinct Fibonacci numbers from the set $\{F_1, F_2, \dots, F_{k-2}, F_k\}$.

In all cases m is a sum of distinct members from the set $\{F_1, F_2, F_3, \dots, F_k\}$, which is $P(k+1)$.

The result follows by the Second Principle of Mathematical Induction.

Appendix: Table of primes

The following table lists all the odd integers up to 3999, excluding the multiples of 5. The entry ‘P’ in the table indicates that the number is prime. Otherwise the smallest prime factor of the number is given. The numbers are arranged in blocks of 100, with the units digit at the head of the column and the number of 10s in the left-hand column.

So, for example, the third row at the start of the table has the value 2 in its left-hand column, and entries 3, P, 3, P under the units digits of 1, 3, 7 and 9 respectively. A left-hand column value of 2 means that there are two 10s. So the first entry of 3 gives the smallest prime factor of the number that is made up of two 10s and the units digit 1, that is, 21. The next entry, which is a P, means that the number that is made up of two 10s and the units digit 3, that is, 23, is prime. The third entry, which is again a 3, means that 3 is the smallest prime factor of 27, and the last entry, which is a P, means that the number 29 is prime.

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
0		P	P	3	50	3	P	3	P	100	7	17	19	P	150	19	3	11	3
1	P	P	P	P	51	7	3	11	3	101	3	P	3	P	151	P	17	37	7
2	3	P	3	P	52	P	P	17	23	102	P	3	13	3	152	3	P	3	11
3	P	3	P	3	53	3	13	3	7	103	P	P	17	P	153	P	3	29	3
4	P	P	P	7	54	P	3	P	3	104	3	7	3	P	154	23	P	7	P
5	3	P	3	P	55	19	7	P	13	105	P	3	7	3	155	3	P	3	P
6	P	3	P	3	56	3	P	3	P	106	P	P	11	P	156	7	3	P	3
7	P	P	7	P	57	P	3	P	3	107	3	29	3	13	157	P	11	19	P
8	3	P	3	P	58	7	11	P	19	108	23	3	P	3	158	3	P	3	7
9	7	3	P	3	59	3	P	3	P	109	P	P	P	7	159	37	3	P	3
10	P	P	P	P	60	P	3	P	3	110	3	P	3	P	160	P	7	P	P
11	3	P	3	7	61	13	P	P	P	111	11	3	P	3	161	3	P	3	P
12	11	3	P	3	62	3	7	3	17	112	19	P	7	P	162	P	3	P	3
13	P	7	P	P	63	P	3	7	3	113	3	11	3	17	163	7	23	P	11
14	3	11	3	P	64	P	P	P	11	114	7	3	31	3	164	3	31	3	17
15	P	3	P	3	65	3	P	3	P	115	P	P	13	19	165	13	3	P	3
16	7	P	P	13	66	P	3	23	3	116	3	P	3	7	166	11	P	P	P
17	3	P	3	P	67	11	P	P	7	117	P	3	11	3	167	3	7	3	23
18	P	3	11	3	68	3	P	3	13	118	P	7	P	29	168	41	3	7	3
19	P	P	P	P	69	P	3	17	3	119	3	P	3	11	169	19	P	P	P
20	3	7	3	11	70	P	19	7	P	120	P	3	17	3	170	3	13	3	P
21	P	3	7	3	71	3	23	3	P	121	7	P	P	23	171	29	3	17	3
22	13	P	P	P	72	7	3	P	3	122	3	P	3	P	172	P	P	11	7
23	3	P	3	P	73	17	P	11	P	123	P	3	P	3	173	3	P	3	37
24	P	3	13	3	74	3	P	3	7	124	17	11	29	P	174	P	3	P	3
25	P	11	P	7	75	P	3	P	3	125	3	7	3	P	175	17	P	7	P
26	3	P	3	P	76	P	7	13	P	126	13	3	7	3	176	3	41	3	29
27	P	3	P	3	77	3	P	3	19	127	31	19	P	P	177	7	3	P	3
28	P	P	7	17	78	11	3	P	3	128	3	P	3	P	178	13	P	P	P
29	3	P	3	13	79	7	13	P	17	129	P	3	P	3	179	3	11	3	7
30	7	3	P	3	80	3	11	3	P	130	P	P	P	7	180	P	3	13	3
31	P	P	P	11	81	P	3	19	3	131	3	13	3	P	181	P	7	23	17
32	3	17	3	7	82	P	P	P	P	132	P	3	P	3	182	3	P	3	31
33	P	3	P	3	83	3	7	3	P	133	11	31	7	13	183	P	3	11	3
34	11	7	P	P	84	29	3	7	3	134	3	17	3	19	184	7	19	P	43
35	3	P	3	P	85	23	P	P	P	135	7	3	23	3	185	3	17	3	11
36	19	3	P	3	86	3	P	3	11	136	P	29	P	37	186	P	3	P	3
37	7	P	13	P	87	13	3	P	3	137	3	P	3	7	187	P	P	P	P
38	3	P	3	P	88	P	P	P	7	138	P	3	19	3	188	3	7	3	P
39	17	3	P	3	89	3	19	3	29	139	13	7	11	P	189	31	3	7	3
40	P	13	11	P	90	17	3	P	3	140	3	23	3	P	190	P	11	P	23
41	3	7	3	P	91	P	11	7	P	141	17	3	13	3	191	3	P	3	19
42	P	3	7	3	92	3	13	3	P	142	7	P	P	P	192	17	3	41	3
43	P	P	19	P	93	7	3	P	3	143	3	P	3	P	193	P	P	13	7
44	3	P	3	P	94	P	23	P	13	144	11	3	P	3	194	3	29	3	P
45	11	3	P	3	95	3	P	3	7	145	P	P	31	P	195	P	3	19	3
46	P	P	P	7	96	31	3	P	3	146	3	7	3	13	196	37	13	7	11
47	3	11	3	P	97	P	7	P	11	147	P	3	7	3	197	3	P	3	P
48	13	3	P	3	98	3	P	3	23	148	P	P	P	P	198	7	3	P	3
49	P	17	7	P	99	P	3	P	3	149	3	P	3	P	199	11	P	P	P

Chapter 2 Prime numbers

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
200	3	P	3	7	250	41	P	23	13	300	P	3	31	3	350	3	31	3	11
201	P	3	P	3	251	3	7	3	11	301	P	23	7	P	351	P	3	P	3
202	43	7	P	P	252	P	3	7	3	302	3	P	3	13	352	7	13	P	P
203	3	19	3	P	253	P	17	43	P	303	7	3	P	3	353	3	P	3	P
204	13	3	23	3	254	3	P	3	P	304	P	17	11	P	354	P	3	P	3
205	7	P	11	29	255	P	3	P	3	305	3	43	3	7	355	53	11	P	P
206	3	P	3	P	256	13	11	17	7	306	P	3	P	3	356	3	7	3	43
207	19	3	31	3	257	3	31	3	P	307	37	7	17	P	357	P	3	7	3
208	P	P	P	P	258	29	3	13	3	308	3	P	3	P	358	P	P	17	37
209	3	7	3	P	259	P	P	7	23	309	11	3	19	3	359	3	P	3	59
210	11	3	7	3	260	3	19	3	P	310	7	29	13	P	360	13	3	P	3
211	P	P	29	13	261	7	3	P	3	311	3	11	3	P	361	23	P	P	7
212	3	11	3	P	262	P	43	37	11	312	P	3	53	3	362	3	P	3	19
213	P	3	P	3	263	3	P	3	7	313	31	13	P	43	363	P	3	P	3
214	P	P	19	7	264	19	3	P	3	314	3	7	3	47	364	11	P	7	41
215	3	P	3	17	265	11	7	P	P	315	23	3	7	3	365	3	13	3	P
216	P	3	11	3	266	3	P	3	17	316	29	P	P	P	366	7	3	19	3
217	13	41	7	P	267	P	3	P	3	317	3	19	3	11	367	P	P	P	13
218	3	37	3	11	268	7	P	P	P	318	P	3	P	3	368	3	29	3	7
219	7	3	13	3	269	3	P	3	P	319	P	31	23	7	369	P	3	P	3
220	31	P	P	47	270	37	3	P	3	320	3	P	3	P	370	P	7	11	P
221	3	P	3	7	271	P	P	11	P	321	13	3	P	3	371	3	47	3	P
222	P	3	17	3	272	3	7	3	P	322	P	11	7	P	372	61	3	P	3
223	23	7	P	P	273	P	3	7	3	323	3	53	3	41	373	7	P	37	P
224	3	P	3	13	274	P	13	41	P	324	7	3	17	3	374	3	19	3	23
225	P	3	37	3	275	3	P	3	31	325	P	P	P	P	375	11	3	13	3
226	7	31	P	P	276	11	3	P	3	326	3	13	3	7	376	P	53	P	P
227	3	P	3	43	277	17	47	P	7	327	P	3	29	3	377	3	7	3	P
228	P	3	P	3	278	3	11	3	P	328	17	7	19	11	378	19	3	7	3
229	29	P	P	11	279	P	3	P	3	329	3	37	3	P	379	17	P	P	29
230	3	7	3	P	280	P	P	7	53	330	P	3	P	3	380	3	P	3	13
231	P	3	7	3	281	3	29	3	P	331	7	P	31	P	381	37	3	11	3
232	11	23	13	17	282	7	3	11	3	332	3	P	3	P	382	P	P	43	7
233	3	P	3	P	283	19	P	P	17	333	P	3	47	3	383	3	P	3	11
234	P	3	P	3	284	3	P	3	7	334	13	P	P	17	384	23	3	P	3
235	P	13	P	7	285	P	3	P	3	335	3	7	3	P	385	P	P	7	17
236	3	17	3	23	286	P	7	47	19	336	P	3	7	3	386	3	P	3	53
237	P	3	P	3	287	3	13	3	P	337	P	P	11	31	387	7	3	P	3
238	P	P	7	P	288	43	3	P	3	338	3	17	3	P	388	P	11	13	P
239	3	P	3	P	289	7	11	P	13	339	P	3	43	3	389	3	17	3	7
240	7	3	29	3	290	3	P	3	P	340	19	41	P	7	390	47	3	P	3
241	P	19	P	41	291	41	3	P	3	341	3	P	3	13	391	P	7	P	P
242	3	P	3	7	292	23	37	P	29	342	11	3	23	3	392	3	P	3	P
243	11	3	P	3	293	3	7	3	P	343	47	P	7	19	393	P	3	31	3
244	P	7	P	31	294	17	3	7	3	344	3	11	3	P	394	7	P	P	11
245	3	11	3	P	295	13	P	P	11	345	7	3	P	3	395	3	59	3	37
246	23	3	P	3	296	3	P	3	P	346	P	P	P	P	396	17	3	P	3
247	7	P	P	37	297	P	3	13	3	347	3	23	3	7	397	11	29	41	23
248	3	13	3	19	298	11	19	29	7	348	59	3	11	3	398	3	7	3	P
249	47	3	11	3	299	3	41	3	P	349	P	7	13	P	399	13	3	7	3

Chapter 3

Congruence

Introduction

It is curious how often seemingly very different branches of mathematics become interlinked by some problem. For more than 2000 years it had been known how to construct both an equilateral triangle and a regular pentagon inscribed in a given circle using only compass and straight edge. But as the seventeenth century drew to its close, constructions were still not known for any other regular polygon with a prime number of sides. The brilliant French mathematician Fermat had been discussing the numbers $F_n = 2^{2^n} + 1$ (later to become known as *Fermat numbers*), believing them all to be prime, unaware of how intricately these numbers were woven into the solution of the polygon problem. It required the genius of the German mathematician Gauss to see how these numbers could be used to solve the construction problem.

You will learn more about Fermat in Chapter 4.

In the final section of the previous chapter we introduced the idea of a remainder sequence, in which numbers were replaced by their remainder on dividing by some natural number n . Observations about the behaviour of the remainder sequence were then projected back to reveal properties of the original number sequence. Gauss used this idea to develop an ‘arithmetic of remainders’, which he then put to work to ease computations in many areas.

You may like to read more about Gauss in the *History Reader* for this topic.

In this chapter we introduce Gauss’s notion of congruence and develop properties of it that will be useful in problem-solving throughout the remainder of the topic. Here we restrict its application to a variety of problems involving remainders and, in particular, to solving linear congruences (which offer a more general way of looking at linear Diophantine equations). Finally, we prove the classical *Chinese Remainder Theorem*, which is concerned with the existence of (and how to find) solutions to a class of problems that can be modelled as a simultaneous system of linear congruences.

Chapter guide

This chapter is set out in four sections, the most substantial of which is the first. Section 2 is the shortest, and is also not used by the final two sections.

1 Properties of congruence

This chapter begins by defining congruence, and establishing some elementary properties that will enable us to carry out basic algebraic manipulations in this setting.

1.1 Definition and basic properties

It has been suggested that the result that p divides $2^{p-1} - 1$, for every odd prime p , was known to Chinese mathematicians over 2000 years ago. But how does one go about confirming instances of this result? If asked to show that $2^{16} - 1$ is divisible by 17 it would be feasible to compute 2^{16} by hand, subtract 1, and then carefully divide by 17. But it would be impractical to try the same line of attack to confirm that 641 divides $2^{640} - 1$ because this number is so huge. You will see in this section that such divisions need not be as frightening as they first seem; we can investigate divisibility without having to do the computations involved in the division. Instead we can use an ‘arithmetic of remainders’ in which everything hinges on the following key definition.

Definition 1.1 Congruence modulo n

Let n be a fixed natural number and let a and b be any integers. We say that a is **congruent to b modulo n** if the difference $a - b$ is divisible by n .

In symbols we write $a \equiv b \pmod{n}$.

If a is not congruent to b modulo n we say that a is **incongruent to b modulo n** and write $a \not\equiv b \pmod{n}$.

If we write $a \equiv b \pmod{n}$ it is to be understood that a and b are integers and n is a natural number, for the statement would not make sense otherwise.

To illustrate the congruence notation, consider the case of modulus $n = 11$. We have

$$3 \equiv 25 \pmod{11}, \text{ since } 3 - 25 = -22 = -2 \times 11,$$

and

$$7 \equiv -26 \pmod{11}, \text{ since } 7 - (-26) = 33 = 3 \times 11.$$

On the other hand, 12 is incongruent to 8 modulo 11, since $12 - 8 = 4$, and 4 is not a multiple of 11.

Exercise 1.1

For each of the following, decide whether the statement is true or false.

- (a) $3 \equiv 29 \pmod{8}$
- (b) $3 \equiv -29 \pmod{8}$
- (c) $63 \equiv 37 \pmod{13}$
- (d) $37 \equiv 63 \pmod{13}$
- (e) $63 \equiv 63 \pmod{37}$
- (f) $63 \not\equiv 13 \pmod{25}$

Parts (c) and (d) of Exercise 1.1 illustrate one apparent property of congruence, namely that if a is congruent to b modulo n then b is

congruent to a modulo n . Part (e) illustrates the further property that any integer is congruent to itself modulo n . These are two of a number of general properties of congruence that highlight certain similarities with ordinary equality, and which we will prove in our first result.

Theorem 1.2 *Properties of congruence*

Let n be a fixed natural number and let a, b, c and d be any integers. Then the following properties hold.

- (a) $a \equiv a \pmod{n}$.
- (b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
- (c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.
- (d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.
- (e) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.
- (f) If $a \equiv b \pmod{n}$ then $a^r \equiv b^r \pmod{n}$, for any integer $r \geq 1$.

Proof

- (a) $a - a = 0 = 0 \times n$, so $a \equiv a \pmod{n}$.
- (b) If $a \equiv b \pmod{n}$ then there exists an integer k such that $a - b = kn$.

Then

$$b - a = -(a - b) = (-k)n,$$

so that $b \equiv a \pmod{n}$.

- (c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then there exist integers s and t such that

$$a - b = sn \quad \text{and} \quad b - c = tn.$$

Adding these two equations gives

$$(a - b) + (b - c) = sn + tn.$$

That is,

$$a - c = (s + t)n,$$

so that $a \equiv c \pmod{n}$.

- (d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then there exist integers s and t such that

$$a - b = sn \quad \text{and} \quad c - d = tn.$$

Adding these two equations gives

$$(a + c) - (b + d) = sn + tn = (s + t)n,$$

so that

$$a + c \equiv b + d \pmod{n}.$$

- (e) With $a - b = sn$ and $c - d = tn$ as in the proof of property (d),

$$ac = (b + sn)(d + tn) = bd + n(bt + sd + stn),$$

and so

$$ac - bd = n(bt + sd + stn),$$

confirming that $ac \equiv bd \pmod{n}$.

- (f) The case $r = 1$ is trivially true. Continuing by induction, suppose the result is true for $r = k$, that is, suppose $a^k \equiv b^k \pmod{n}$ whenever $a \equiv b \pmod{n}$.

Then

$$\begin{aligned} a^{k+1} &= aa^k \equiv bb^k \pmod{n}, & \text{by property (e),} \\ &\equiv b^{k+1} \pmod{n}. \end{aligned}$$

This confirms the truth of the case $r = k + 1$ and completes the induction step. The result follows by mathematical induction. ■

The following exercise gives you an opportunity to prove some simple properties of congruence by working from the definition alone.

Exercise 1.2

Suppose that $a \equiv b \pmod{n}$ and m is an integer. Prove the following.

- (a) If $m > 0$ and m divides n then $a \equiv b \pmod{m}$.
- (b) If $m > 0$ then $ma \equiv mb \pmod{mn}$ and $ma \equiv mb \pmod{n}$.
- (c) If $d > 0$ is a common factor of a , b and n , then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.
- (d) $\text{hcf}(a, n) = \text{hcf}(b, n)$.
- (e) For any integer c , $a + c \equiv b + c \pmod{n}$.

Before developing further ideas, let us illustrate a range of problems in which properties of congruence can be exploited to ease computation.

Worked Exercise 1.3

Show that $37^{37} + 2$ is divisible by 13.

Solution

We start by looking for numbers to which 37^{37} is congruent modulo 13. Now as $37 \equiv -2 \pmod{13}$, Theorem 1.2(f) tells us that

$$37^{37} \equiv (-2)^{37} \equiv (-1) \times 2^{37} \pmod{13}.$$

Now

$$2^4 = 16 \equiv 3 \pmod{13},$$

and so

$$37^{37} \equiv (-1) \times (2^4)^9 \times 2 \equiv (-1) \times 3^9 \times 2 \pmod{13}.$$

But

$$3^3 = 27 \equiv 1 \pmod{13},$$

so

$$37^{37} \equiv 3^3 \times 3^3 \times 3^3 \times (-2) \equiv -2 \pmod{13}.$$

Finally, Theorem 1.2(d) allows us to conclude that

$$37^{37} + 2 \equiv (-2) + 2 \equiv 0 \pmod{13},$$

which amounts to saying that $37^{37} + 2$ is divisible by 13.

In the final step of Worked Exercise 1.3 we inferred from a statement of the form $a \equiv 0 \pmod{n}$ that n divides a . This is an immediate consequence of the definition of congruence. Indeed, we have a characterisation of congruence modulo n in terms of the remainders on dividing by n , as given by the following proposition.

Proposition 1.4 *Congruent integers have the same remainders*

$a \equiv b \pmod{n}$ if, and only if, the integers a and b have the same remainder when divided by n .

Proof Suppose first that a and b have the same remainder when divided by n , say

$$a = q_1n + r \quad \text{and} \quad b = q_2n + r, \quad \text{where } 0 \leq r < n.$$

Then $a - b = (q_1 - q_2)n$, showing that $a \equiv b \pmod{n}$.

Conversely, suppose that $a \equiv b \pmod{n}$, so that $a - b = kn$, for some integer k . Let b have remainder r when divided by n , so that $b = nq + r$ for some integer q . Then

$$a = b + kn = nq + r + kn = (q + k)n + r$$

shows that a has the same remainder, r , as b . ■

1.2 Residue classes

One outcome of Proposition 1.4 is that every integer is congruent to exactly one of the integers $0, 1, 2, \dots, n - 1$ modulo n , namely whichever one of these is its remainder on dividing by n . This set of n integers is called the set of **least positive residues** modulo n . (Strictly speaking, since 0 is not a positive integer, it ought to be called the set of *least non-negative residues*, but this misnomer is firmly entrenched in the literature.)

Furthermore, we can split up $\mathbb{Z}$ into non-overlapping sets called **residue** (or **congruence**) **classes**, where two integers belong to the same class if, and only if, they are congruent modulo n . For example, for the case $n = 4$ the residue classes are as follows.

$$\begin{aligned} &\{\dots, -8, -4, 0, 4, 8, \dots\} \\ &\{\dots, -7, -3, 1, 5, 9, \dots\} \\ &\{\dots, -6, -2, 2, 6, 10, \dots\} \\ &\{\dots, -5, -1, 3, 7, 11, \dots\} \end{aligned}$$

A set obtained by selecting one member from each of these residue classes, for example $\{0, 1, 2, 3\}$ or $\{8, -3, 22, -9\}$, is called a **complete set of residues** modulo 4. In general, a set $\{a_1, a_2, a_3, \dots, a_n\}$ of n integers is a complete set of residues modulo n provided no two of them are congruent modulo n . By virtue of Proposition 1.4 this will mean that the integers $\{a_1, a_2, a_3, \dots, a_n\}$ are congruent, in some order, to $\{0, 1, 2, \dots, n - 1\}$ modulo n .

In choosing a complete set of residues modulo n , our most frequent selection will be the set of least positive residues, $\{0, 1, 2, \dots, n - 1\}$. However, we will have occasion to use the set of **least absolute residues** obtained by choosing, from each residue class, the one with least modulus. To be precise, from each residue class modulo n we choose the unique member x that lies in the range $-\frac{1}{2}n < x \leq \frac{1}{2}n$. For example, the set of least absolute residues for $n = 4$ is $\{-1, 0, 1, 2\}$ whilst for $n = 7$ it is $\{-3, -2, -1, 0, 1, 2, 3\}$.

Exercise 1.3

- (a) Write down the set of least positive residues modulo n , and the set of least absolute residues modulo n , for (i) $n = 10$ and (ii) $n = 11$.
- (b) Determine whether or not each of the following sets is a complete set of residues modulo 11.
- (i) $\{6, 2, -3, 22, 23, -7, 7, 9, 43, -8, 16\}$
 - (ii) $\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2\}$
 - (iii) $\{0, 1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$

Properties (d) and (e) of Theorem 1.2 are of great importance. In essence they say that the residue class to which a sum $a + c$, or a product ac , belongs does not depend on the individual numbers a and c , but rather on the residue classes to which they belong. To clarify this remark, let us denote by $[r]$ the residue class modulo n to which the integer r belongs. So

$$[r] = \{\dots, r - 2n, r - n, r, r + n, r + 2n, \dots\}.$$

This will mean that residue classes are denoted in many different ways; for example when $n = 5$, $[-1] = [4] = [19]$ since $-1 \equiv 4 \equiv 19 \pmod{5}$. In this notation, properties (d) and (e) can be restated as follows.

(d) If $[a] = [b]$ and $[c] = [d]$ then $[a + c] = [b + d]$.

(e) If $[a] = [b]$ and $[c] = [d]$ then $[ac] = [bd]$.

These two facts amount to saying that the operations defined by

$$[a] + [c] = [a + c] \text{ and } [a] \times [c] = [ac]$$

on the set of residue classes modulo n are unambiguous. Whatever numbers are chosen to represent the two residue classes, the sum of the numbers will always belong to the same class, as will the product of the numbers.

Let

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

be the set of all residue classes modulo n . Together with the operations of addition and multiplication defined above, we have an arithmetic on $\mathbb{Z}_n$.

For example, taking $n = 4$ we have the tables

+	[0]	[1]	[2]	[3]	×	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[0]	[1]	[0]	[1]	[2]	[3]
[2]	[2]	[3]	[0]	[1]	[2]	[0]	[2]	[0]	[2]
[3]	[3]	[0]	[1]	[2]	[3]	[0]	[3]	[2]	[1]

where, for example, $[3] \times [2] = [2]$ is obtained from the definition

$$[3] \times [2] = [3 \times 2] = [6]$$

and the fact that $[6] = [2]$ since $6 \equiv 2 \pmod{4}$.

Exercise 1.4

Working in $\mathbb{Z}_{10}$, determine $[6] + [8]$ and $[6] \times [8]$ and find all $[b]$ such that $[6] \times [b] = [8]$.

Repeat the above, this time working in $\mathbb{Z}_{11}$.

A problem in congruence modulo n is equivalent to a problem in $\mathbb{Z}_n$ with its arithmetic as illustrated in Exercise 1.4 above. In practice, however, we abandon much of this formalism. What we will do is select a complete set of residues (usually the set of least positive residues) and work with these numbers, dropping the square brackets. When any sum or product is calculated we replace the answer with the chosen residue to which it is congruent. Here are a couple of illustrations of the way in which congruence is used.

Worked Exercise 1.5

- (a) Show that $1^3 + 2^3 + 3^3 + \cdots + 60^3$ is divisible by 5.
- (b) Show that there do not exist integers x and y such that $x^2 + y^2 = 999$.

Solution

- (a) In terms of congruence we are asked to show that $1^3 + 2^3 + 3^3 + \cdots + 60^3$ is congruent to 0 modulo 5. Now each of the terms r^3 is congruent to one of 0, 1, 2, 3 or 4 modulo 5, and so one line of attack would be to evaluate the least positive residue modulo 5 of each of these cubes and add up. However, a considerable shortcut is provided by Theorem 1.2(f), which tells us that if two numbers are congruent modulo 5 then their cubes are also congruent modulo 5. So, since $1 \equiv 6 \equiv 11 \equiv \cdots \equiv 56 \pmod{5}$, we have

$$1^3 \equiv 6^3 \equiv 11^3 \equiv \cdots \equiv 56^3 \pmod{5}.$$

Similarly

$$2^3 \equiv 7^3 \equiv 12^3 \equiv \cdots \equiv 57^3 \pmod{5},$$

$$3^3 \equiv 8^3 \equiv 13^3 \equiv \cdots \equiv 58^3 \pmod{5},$$

$$4^3 \equiv 9^3 \equiv 14^3 \equiv \cdots \equiv 59^3 \pmod{5},$$

$$5^3 \equiv 10^3 \equiv 15^3 \equiv \cdots \equiv 60^3 \pmod{5}.$$

Therefore,

$$1^3 + 2^3 + 3^3 + \cdots + 60^3 \\ \equiv 12 \times (1^3 + 2^3 + 3^3 + 4^3 + 5^3) \pmod{5}.$$

Now,

$$2^3 = 8 \equiv 3, \quad 3^3 = 27 \equiv 2, \quad 4^3 = 64 \equiv 4 \\ \text{and } 5^3 \equiv 0^3 \equiv 0 \pmod{5},$$

and so

$$1^3 + 2^3 + 3^3 + \cdots + 60^3 \equiv 12 \times (1 + 3 + 2 + 4 + 0) = 120 \\ \equiv 0 \pmod{5},$$

as claimed.

- (b) At first glance it might be difficult to see what this question has to do with congruence. In fact, it is a particular case of a general result concerning the possible values that a sum of two squares can take modulo 4.

Any integer x is congruent to one of the integers 0, 1, 2 or 3 modulo 4. Theorem 1.2(f) tells us that x^2 is therefore congruent to one of the numbers 0^2 , 1^2 , 2^2 or 3^2 modulo 4. That is, x^2 is congruent to either 0 or 1 modulo 4 (since $2^2 \equiv 0 \pmod{4}$ and $3^2 \equiv 1 \pmod{4}$). Similarly, for any integer y , y^2 is congruent to either 0 or 1 modulo 4. Theorem 1.2(d) now gives

$$x^2 + y^2 \equiv 0, 1 \text{ or } 2 \pmod{4}$$

(as 0, 1 and 2 are the possible results of adding either 0 or 1 to either 0 or 1).

This argument tells us that any integer that is congruent to 3 modulo 4 cannot be written as the sum of two squares. Now $999 \equiv 3 \pmod{4}$ is such an integer, and so the equation

$$x^2 + y^2 = 999$$

cannot have a solution in integers.

There are simpler ways of solving Worked Exercise 1.5(a).

For instance, you may be familiar with the formula

$$\sum_{r=1}^n r^3 = \left(\frac{n(n+1)}{2} \right)^2,$$

in which case you could deduce the result by putting $n = 60$.

Our solution here intentionally illustrates the use of the properties of congruence.

And now some problems for you to solve.

Exercise 1.5

- (a) What is the remainder when $1! + 2! + 3! + \cdots + 1000!$ is divided by 7?
 (b) Let a be an integer that is not divisible by either 2 or 3. Prove that $a^2 - 1$ is divisible by 24.

Hint: show $a^2 \equiv 1 \pmod{24}$.

1.3 Further properties

There is a property of congruence that, although it is no more than a re-expression of an established divisibility property, will be used so often that it merits the status of a theorem.

Theorem 1.6

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then

$$a \equiv b \pmod{\text{lcm}(m, n)}.$$

Proof From the definition of congruence there exist integers r and s such that

$$a - b = rm \quad \text{and} \quad a - b = sn.$$

Let $d = \text{hcf}(m, n)$, so that

$$m = dm' \quad \text{and} \quad n = dn', \quad \text{where } \text{hcf}(m', n') = 1.$$

Substituting for m and n in the equation $rm = sn$ gives

$$rdm' = sdn'; \quad \text{that is, } rm' = sn'.$$

We infer from this that n' divides rm' , whereupon Euclid's Lemma gives us that n' divides r . So putting $r = kn'$ we have

$$a - b = rm = kmn' = km \left(\frac{n}{d}\right) = k \left(\frac{mn}{d}\right) = k \text{lcm}(m, n).$$

That is, $a \equiv b \pmod{\text{lcm}(m, n)}$, as claimed. ■

One particular case of Theorem 1.6 is well worth highlighting. We will frequently want to apply this result when m and n are coprime, in which case $\text{lcm}(m, n) = mn$.

Corollary 1.7 to Theorem 1.6

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where $\text{hcf}(m, n) = 1$, then $a \equiv b \pmod{mn}$.

Notice how much simpler Exercise 1.5(b) would have been with the benefit of Theorem 1.6. To show that $a^2 \equiv 1 \pmod{24}$ it is sufficient to show that $a^2 \equiv 1 \pmod{8}$ and $a^2 \equiv 1 \pmod{3}$. Both these separate parts are quickly confirmed from congruence ideas:

(1) a odd implies $a \equiv 1, 3, 5$ or $7 \pmod{8}$, and squaring,

$$a^2 \equiv 1 \pmod{8} \text{ in all cases;}$$

(2) a not divisible by 3 implies $a \equiv 1$ or $2 \pmod{3}$, and squaring,

$$a^2 \equiv 1 \pmod{3} \text{ in each case.}$$

We have seen that if $a \equiv b \pmod{n}$ then $ca \equiv cb \pmod{n}$, for any integer c . What about the converse of this result? If $ca \equiv cb \pmod{n}$ can we

Proposition 4.10 of Chapter 1 establishes that $\text{hcf}(m', n') = 1$.

See Proposition 4.15 of Chapter 1.

legitimately cancel the cs to recover $a \equiv b \pmod{n}$? In fact we cannot, as this simple counter-example shows:

$$2 \equiv 8 \pmod{6} \text{ but } 1 \not\equiv 4 \pmod{6}.$$

Here, cancellation of the common factor 2 has produced a contradiction.

Common factors on two sides of a congruence can always be cancelled, but in doing so the modulus has to be adjusted according to the following rule.

Proposition 1.8 Cancellation Rule

If $ca \equiv cb \pmod{n}$ then $a \equiv b \pmod{\frac{n}{d}}$, where $d = \text{hcf}(c, n)$.

Proof From $ca \equiv cb \pmod{n}$ we know that there exists an integer k such that $ca - cb = kn$. Now $\text{hcf}(c, n) = d$, and so there exist coprime integers r and s such that $c = dr$ and $n = ds$. Therefore, substituting for c and n in the equation $ca - cb = kn$ gives

$$dra - drb = kds,$$

which, after cancelling the common d , gives

$$r(a - b) = ks.$$

From this s divides $r(a - b)$ and, as $\text{hcf}(r, s) = 1$, Euclid's Lemma confirms that s divides $a - b$. Consequently $a \equiv b \pmod{s}$, where $s = \frac{n}{d}$. ■

Proposition 4.10 of Chapter 1 established that r and s are coprime.

Let us revisit the counter-example from before the proposition. Given $2 \equiv 8 \pmod{6}$, we see that $\text{hcf}(2, 6) = 2$, so we can cancel the 2 by also dividing the modulus by 2. Thus $1 \equiv 4 \pmod{3}$.

One special case of Proposition 1.8 is worth noting: when $\text{hcf}(c, n) = 1$ the common factor c can be cancelled without the need to adjust the modulus. This is stated formally as follows.

Corollary 1.9 to the Cancellation Rule

If $ca \equiv cb \pmod{n}$, where $\text{hcf}(c, n) = 1$, then $a \equiv b \pmod{n}$.

In fact, the two congruences in Proposition 1.8 are 'equivalent' because the reverse implication also holds. That is,

$$\text{if } a \equiv b \pmod{\frac{n}{d}} \text{ then } ca \equiv cb \pmod{n}, \text{ where } d = \text{hcf}(c, n).$$

To justify this remark, suppose that $a \equiv b \pmod{\frac{n}{d}}$. Then there is an integer k such that

$$a - b = k\frac{n}{d}.$$

Multiplying by c gives

$$ca - cb = \frac{kc}{d}n,$$

so that $ca \equiv cb \pmod{n}$, since $\frac{c}{d}$ is an integer.

For example, the congruence $12x \equiv 18 \pmod{27}$ can be simplified by cancellation of the common factor 6 and dividing the modulus by $\text{hcf}(6, 27) = 3$. So if $12x \equiv 18 \pmod{27}$ then $2x \equiv 3 \pmod{9}$ by the Cancellation Rule.

Conversely, if $2x \equiv 3 \pmod{9}$ then, as argued above, we also have $12x \equiv 18 \pmod{27}$. We make use of the symbol $\iff$ (pronounced in this context as ‘is equivalent to’) to indicate that two congruences are ‘equivalent’. Thus we can write

$$12x \equiv 18 \pmod{27} \iff 2x \equiv 3 \pmod{9}.$$

The congruences are **equivalent** in the sense that an integer x is a solution of one congruence if, and only if, it is a solution of the other.

Exercise 1.6

Use an appropriate cancellation to simplify each of the following congruences:

- (a) $6x \equiv 18 \pmod{30}$
- (b) $20x \equiv 30 \pmod{45}$
- (c) $52x \equiv 39 \pmod{60}$.

Before we leave this area of congruence properties there is one final result that merits our attention. Euclid’s Lemma for the case of a prime factor p showed that if p divides ab , then either p divides a or p divides b . When this is expressed in congruence notation we have the result that follows. We will have numerous occasions to refer to this result so, to ease identification of the reference, we will continue to call it Euclid’s Lemma for prime factors.

Theorem 1.10 *Euclid’s Lemma for prime factors*

If $ab \equiv 0 \pmod{p}$ then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Exercise 1.7

- (a) Determine the least positive residue and the least absolute residue of 1997:
- (i) modulo 7
 - (ii) modulo 17
 - (iii) modulo 101.
- (b) Suppose that $k \equiv 1 \pmod{12}$ for some integer k . What is the least positive residue of $6k + 5$:
- (i) modulo 4
 - (ii) modulo 9
 - (iii) modulo 12?
- (c) (i) Give an example to show that $a^k \equiv b^k \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.
- (ii) Give an example to show that $a^k \equiv b^k \pmod{n}$ and $k \equiv j \pmod{n}$ both being true does not necessarily imply that $a^j \equiv b^j \pmod{n}$ is true.
- (d) Prove by induction that $6^n \equiv 5n + 1 \pmod{25}$, for all integers $n \geq 1$.
- (e) Prove that if $n \geq 2$ and $\text{hcf}(a, n) = 1$ then the set of integers
- $$\{c, c + a, c + 2a, c + 3a, \dots, c + (n - 1)a\}$$
- is a complete set of residues modulo n for any integer c .
- (f) What is the remainder when 11^{11} is divided by:
- (i) 7
 - (ii) 17
 - (iii) 19?
- (g) Use ideas of congruence to prove that:
- (i) 29 divides $2^{28} - 1$
 - (ii) 79 divides $3^{39} + 1$.
- (h) In 1659 Fermat asserted that no prime number of the form $3k - 1$ can be written in the form $a^2 + 3b^2$. Use congruence modulo 3 to show that he was correct.
- (i) From the definition of congruence alone, prove the following.
If $ar \equiv b \pmod{n}$ and $cr \equiv d \pmod{n}$, for some integer r , then $ad \equiv bc \pmod{n}$.

In Exercise 1.3 we have made a start at solving congruence problems. We will return to this in Section 3, but first, in Section 2, we take a short detour.

2 Divisibility tests

Given any integer written in our familiar decimal representation, we can tell at a glance whether or not it is divisible by 2 or 5. To test divisibility by 5, for example, we simply look to see whether or not the units digit is 0 or 5. Though not quite so immediate, there are also fairly simple tests for divisibility by 3, 4, 8, 9 and 11. All these divisibility tests can be derived from congruence ideas.

Historically, the most significant divisibility test is that for division by 9.

A natural number is divisible by 9 if, and only if, the sum of its digits is divisible by 9.

In fact this is a special case of a stronger result, which we will prove shortly.

A natural number is congruent to the sum of its digits modulo 9.

For example, if $N = 974064$ then

$$N \equiv 9 + 7 + 4 + 0 + 6 + 4 = 30 \equiv 3 \pmod{9}.$$

This fact led to a method of checking calculations, known as ‘casting out nines’, which, over the years, has been much used by bookkeepers. The method amounts to reworking the calculations in the residue class arithmetic $\mathbb{Z}_9$. As an illustration, consider the multiplication shown in Figure 2.1. On the left the multiplication is carried out fully, whilst on the right the same calculation is carried out modulo 9.

$ \begin{array}{r} 1489 \\ \times 753 \\ \hline 1042300 \\ 74450 \\ 4467 \\ \hline 1121217 \end{array} $	$ \begin{aligned} 1 + 4 + 8 + 9 &= 22 \equiv 4 \pmod{9} \\ 7 + 5 + 3 &= 15 \equiv 6 \pmod{9} \\ 4 \times 6 &= 24 \equiv 6 \pmod{9} \\ \text{Check: } 1 + 1 + 2 + 1 + 2 + 1 + 7 &= 15 \equiv 6 \pmod{9} \end{aligned} $
---	---

Figure 2.1 Casting out nines

The fact that the two answers agree modulo 9 is far from being conclusive proof that the calculation is correct. However, there is a good chance that a mistake in carrying out the calculation would have shown up during this check.

In the following proposition we prove the results that give divisibility tests for 9 and 11 together.

Proposition 2.1 *Divisibility by 9 and 11*

Let the integer N be written in decimal notation as $N = a_m a_{m-1} \dots a_2 a_1 a_0$ so that the digits satisfy $0 \leq a_i \leq 9$ with $a_m \neq 0$. Then:

- (a) $N \equiv a_0 + a_1 + a_2 + a_3 + \dots + a_m \pmod{9}$
- (b) $N \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m a_m \pmod{11}$.

Proof The key is to write out the number N in terms of powers of 10, namely

$$N = a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \dots + 10^m a_m.$$

- (a) Since $10 \equiv 1 \pmod{9}$, it follows from Theorem 1.2(f) that $10^r \equiv 1 \pmod{9}$ for all integers $r \geq 1$. Thus, from properties (d) and (e) of Theorem 1.2,

$$\begin{aligned} N &\equiv a_0 + 1a_1 + 1a_2 + 1a_3 + \dots + 1a_m \pmod{9} \\ &\equiv a_0 + a_1 + a_2 + a_3 + \dots + a_m \pmod{9}. \end{aligned}$$

- (b) Similarly, since $10 \equiv -1 \pmod{11}$, $10^r \equiv (-1)^r \pmod{11}$ for all integers r and

$$\begin{aligned} N &\equiv a_0 + (-1)a_1 + (-1)^2a_2 + \dots + (-1)^m a_m \pmod{11} \\ &\equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m a_m \pmod{11}. \quad \blacksquare \end{aligned}$$

In the congruences of parts (a) and (b) of Proposition 2.1, and in their proofs, we have unnecessarily used the digits of N in reverse order, starting at the units digit a_0 . It will be helpful to use formula (b) in this way, starting at the positive units digit and then alternating the signs. But in using formula (a) we will often, as we did in Figure 2.1 above, add the digits in their naturally occurring order.

The two special cases in which $N \equiv 0$ in parts (a) and (b) of Proposition 2.1 can be restated as the following result.

Corollary 2.2 *to Proposition 2.1*

- (a) A natural number N is divisible by 9 if, and only if, the sum of its digits is divisible by 9.
- (b) A natural number N is divisible by 11 if, and only if, the alternating sum of its digits is divisible by 11, where by ‘alternating sum’ we mean the sum using alternating signs as given in part (b) of Proposition 2.1.

The following well-known test for division by 3 follows from part (a) of Proposition 2.1.

Proposition 2.3

A natural number N is divisible by 3 if, and only if, the sum of its digits is divisible by 3.

Proof First we show that if N is divisible by 3, then the sum of its digits is divisible by 3. Let N be divisible by 3, that is, $N = 3s$, for some natural number s . Substituting $3s$ for N in Proposition 2.1(a) gives $3s \equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_m \pmod{9}$, which, by the definition of congruence, means that there is an integer t such that

$$a_0 + a_1 + a_2 + a_3 + \cdots + a_m - 3s = 9t.$$

It follows that

$$a_0 + a_1 + a_2 + a_3 + \cdots + a_m = 3s + 9t = 3(s + 3t),$$

which shows that the digit sum is divisible by 3.

Conversely, suppose that the digit sum of N is divisible by 3, that is, the digit sum is equal to $3s$ for some natural number s . Substituting $3s$ for the digit sum in the congruence of Proposition 2.1(a) now gives $N \equiv 3s \pmod{9}$. It follows that $N - 3s = 9t$ for some integer t . Hence

$$N = 3s + 9t = 3(s + 3t),$$

which shows that N is divisible by 3. ■

Exercise 2.1

- (a) Let $N = 9723$ and $M = 18\,056$.
- (i) Determine the remainders when each of the numbers N , M , $N + M$ and $N - M$ is divided by 9.
 - (ii) Determine the remainders when each of the numbers N , M , $N + M$ and $N - M$ is divided by 11.
 - (iii) Determine the missing digit (?) in the product

$$N \times M = 9723 \times 18\,056 = 175(?)58\,488$$

without using a calculator.

- (b) An integer N has an even number of digits. A second integer M is formed by moving the last digit of N to the front. (For example, if $N = 588\,471$ then the 1 is moved to the front, giving $M = 158\,847$.) Show that 9 divides $N - M$, 11 divides $N + M$ and 99 divides $N^2 - M^2$.

There are numerous variations on the following trick, which capitalises on the connection between a number and the sum of its digits. A person is asked to think of any 3-digit number (that is not palindromic). Without knowing what the number is, a prediction is made that application of the

following sequence of operations on the number will produce the answer 1089.

Write down the number and the number formed by reversing the order of its digits. Then subtract the smaller of these numbers from the larger. Finally add to this the number formed by reversing its digits.

For example, if the chosen number is 638 then this is subtracted from 836, giving 198. Adding 198 to 891 gives 1089. The work of this section should enable you to explain why this is so: using an argument similar to that in part (b) of the above exercise should allow you to deduce that the subtraction always gives a number that is divisible by 99. This fact restricts the values that the three digits of this number can take and the result follows.

It may happen that the first subtraction produces a 2-digit number. This is treated as a 3-digit number with leading 0 for the purposes of reversing its digits. For example, 99 would reverse to 990.

Exercise 2.2

- (a) Without carrying out the multiplication, find the missing digit (?) in each of the following products.
- (i) $108 \times 371 = 400(?)8$
 - (ii) $1578 \times 34971 = 5518(?)238$
 - (iii) $4473 \times 3(?)9 = 1426887$
- Hint:* for part (iii), test for divisibility by 11.
- (b) A and B are two different 7-digit numbers, each involving all seven of the digits 1, 2, 3, 4, 5, 6 and 7. Prove that A does not divide B .
- (c) Let $N > M$ be two 10-digit numbers formed from the same 10 digits but in different orders. If X is the sum of the digits of $N - M$, show that the sum of the digits of X is 9.
- (d) Show that 2^n divides an integer N if, and only if, 2^n divides the number made up of the last n digits of N .
- (e) (i) Show that, for all $n \geq 0$, $10^{2n} \equiv 1 \pmod{99}$ and $10^{2n+1} \equiv 10 \pmod{99}$.

- (ii) The remainder on dividing a number by 99 can be found in a way similar to the corresponding result for division by 9, but treating the digits of the number two at a time. The following examples illustrate the method:

$$6239 \equiv 62 + 39 = 101 \equiv 2 \pmod{99}$$

and

$$54787 \equiv 5 + 47 + 87 = 139 \equiv 40 \pmod{99}.$$

Use the result in part (i) to show why this test works.

- (iii) Find a test for divisibility by 101 and use it to determine the remainders when 62479 and 9850833 are divided by 101.

3 Linear congruences

Having studied basic properties of congruence, the next step is to look at the problem of solving congruences involving unknowns, such as $3x \equiv 7 \pmod{12}$ or $x^5 - x^3 \equiv 0 \pmod{8}$. The first of these examples happens to have no solutions, for there is no integer x for which $3x \equiv 7 \pmod{12}$. On the other hand, every integer x satisfies $x^5 - x^3 \equiv 0 \pmod{8}$ – try one!

3.1 Polynomial congruences

By an **integral polynomial** we mean a polynomial

$$P(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$$

in which the coefficients $c_0, c_1, \dots, c_m$ and the variable x are integers. If $P(x)$ is an integral polynomial then the congruence $P(x) \equiv 0 \pmod{n}$ is a **polynomial congruence**. Our present interest is in solving polynomial congruences and we show straight away that if an integer a is a solution of the congruence, that is, $P(a) \equiv 0 \pmod{n}$, then so too is every integer in the residue class of a modulo n .

Proposition 3.1

Let $P(x)$ be an integral polynomial. If $a \equiv b \pmod{n}$ then $P(a) \equiv P(b) \pmod{n}$. In particular, a is a solution of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ if, and only if, b is a solution.

Proof Let $P(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$. Since $a \equiv b \pmod{n}$, properties (e) and (f) of Theorem 1.2 of this chapter tell us that $c_r a^r \equiv c_r b^r \pmod{n}$, for each integer $r \geq 1$. Property (d) of Theorem 1.2 then gives

$$\begin{aligned} P(a) &= c_m a^m + c_{m-1} a^{m-1} + \cdots + c_1 a + c_0 \\ &\equiv c_m b^m + c_{m-1} b^{m-1} + \cdots + c_1 b + c_0 \equiv P(b) \pmod{n}. \end{aligned}$$

In particular, $P(a) \equiv 0 \pmod{n}$ if, and only if, $P(b) \equiv 0 \pmod{n}$. That is, a is a solution of the congruence $P(x) \equiv 0 \pmod{n}$ if, and only if, b is a solution. ■

As a consequence of Proposition 3.1, it is apparent that the problem of solving the congruence $P(x) \equiv 0 \pmod{n}$ is really a problem in the residue class arithmetic $\mathbb{Z}_n$; if an integer is a solution then so too is every integer in its residue class. So the task is to find which residue classes solve the congruence. Two congruent integers that satisfy a polynomial congruence will be thought of as being the *same* solution.

Definition 3.2 *Number of solutions of a polynomial congruence*

Let $S = \{b_1, b_2, \dots, b_n\}$ be a complete set of residues modulo n . The *number of solutions* of the congruence $P(x) \equiv 0 \pmod{n}$ is the number of integers $b \in S$ for which $P(b) \equiv 0 \pmod{n}$.

Here is an example.

Worked Exercise 3.3

Solve the polynomial congruence $x^2 - x \equiv 0 \pmod{6}$.

Solution

There are six residue classes modulo 6 and each may be a solution of the congruence. We choose the least positive residues, 0, 1, 2, 3, 4 and 5, and test each one in turn.

$$0^2 - 0 \equiv 0 \pmod{6}$$

$$1^2 - 1 \equiv 0 \pmod{6}$$

$$2^2 - 2 \equiv 2 \pmod{6}$$

$$3^2 - 3 \equiv 0 \pmod{6}$$

$$4^2 - 4 \equiv 0 \pmod{6}$$

$$5^2 - 5 \equiv 2 \pmod{6}$$

We see that 0, 1, 3 and 4 are solutions of the congruence and therefore so too is any integer congruent to one of 0, 1, 3 or 4 modulo 6. On the other hand, any integer that is congruent to either 2 or 5 modulo 6 does not satisfy the congruence. The congruence has *four* solutions:

$$x \equiv 0, 1, 3, 4 \pmod{6}.$$

Exercise 3.1

Solve the following polynomial congruences.

(a) $P_1(x) = x^2 + 3x + 4 \equiv 0 \pmod{7}$

(b) $P_2(x) = x^4 - 1 \equiv 0 \pmod{5}$

This method of solving a problem by checking every possible candidate is called **solution by exhaustion**.

3.2 Linear congruences

We have quickly found an algorithmic method for solving polynomial congruences – namely, substitute for x , in turn, each value from any complete set of residues and record the resulting zeros. This is all well and good when the modulus in question is reasonably small and the degree of the polynomial is not too large. For more awkward polynomials the amount of computation involved in this sledgehammer attack quickly renders it impractical, and we must look around for something more subtle. In Chapter 4 we return to the problem of solving general polynomial congruences. There you will discover ways of simplifying polynomial congruences and will learn to predict how many solutions a given polynomial congruence has. Book C, Chapter 10 is concerned with quadratic congruences and their solutions. For the remainder of this chapter we confine our attention to the linear congruence

$$ax \equiv b \pmod{n}.$$

This, the simplest of all polynomial congruences, crops up naturally in a variety of situations in number theory.

Suppose that x_0 is an integer such that $ax_0 \equiv b \pmod{n}$. This means that n divides $ax_0 - b$ or, put another way, there exists an integer y_0 such that

$$ax_0 - b = ny_0.$$

Rearranging this equation tells us that $x = x_0, y = y_0$ is a solution of the linear Diophantine equation $ax - ny = b$. On the other hand if $x = x_0, y = y_0$ is any solution of $ax - ny = b$ then it is certainly the case that $ax_0 \equiv b \pmod{n}$. Thus the problem of finding all integers satisfying the linear congruence $ax \equiv b \pmod{n}$ is precisely the same problem as finding all x -values in solutions of the linear Diophantine equation $ax - ny = b$. As we have already solved the latter problem in Theorem 5.4 of Chapter 1, our principal result on linear congruences is little more than a re-expression of that earlier theorem.

Theorem 3.4 *Solution of linear congruences*

Consider the linear congruence $ax \equiv b \pmod{n}$.

- (a) The congruence has solutions if, and only if, $\text{hcf}(a, n)$ divides b .
- (b) If $\text{hcf}(a, n) = 1$, the congruence has a unique solution.
- (c) If $\text{hcf}(a, n) = d$ and d divides b , then the congruence has d solutions, which are given by the unique solution modulo $\frac{n}{d}$ of the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

Proof

- (a) The linear Diophantine equation $ax - ny = b$ has solutions if, and only if, $\text{hcf}(a, n)$ divides b . From the remarks preceding the theorem, it follows that the congruence $ax \equiv b \pmod{n}$ has solutions if, and only if, $\text{hcf}(a, n)$ divides b .
- (b) Suppose that $\text{hcf}(a, n) = 1$. Theorem 5.4 of Chapter 1 tells us that if $x = x_0, y = y_0$ is one solution of $ax - ny = b$, then the general solution is

$$x = x_0 + nk, \quad y = y_0 + ak, \quad k \in \mathbb{Z}.$$

But for all integers k

$$x_0 + nk \equiv x_0 \pmod{n}$$

and so $x \equiv x_0 \pmod{n}$ is the only solution of $ax \equiv b \pmod{n}$.

- (c) If $\text{hcf}(a, n) = d$ and d divides b then

$$ax \equiv b \pmod{n} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

But $\text{hcf}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, and so the right-hand congruence has a unique solution modulo $\frac{n}{d}$, say

$$x \equiv x_1 \pmod{\frac{n}{d}}.$$

Hence the integers x that satisfy $ax \equiv b \pmod{n}$ are precisely those of the form $x = x_1 + k\frac{n}{d}$, for some integer k .

Consider the set of d integers

$$\left\{x_1, x_1 + \frac{n}{d}, x_1 + 2\frac{n}{d}, \dots, x_1 + (d-1)\frac{n}{d}\right\}.$$

Certainly no two of these integers are congruent modulo n , because they are distinct and no two differ by as much as n . We claim further that, for any integer k , $x_1 + k\frac{n}{d}$ is congruent to one of them modulo n . To see why that is so, write $k = dq + r$, where $0 \leq r < d$, as given by the Division Algorithm. Then

$$\begin{aligned} x_1 + k\frac{n}{d} &= x_1 + (dq + r)\frac{n}{d} = x_1 + nq + r\frac{n}{d} \\ &\equiv x_1 + r\frac{n}{d} \pmod{n}. \end{aligned}$$

So these are the d solutions of $ax \equiv b \pmod{n}$. ■

To illustrate part (c) and its proof, consider the congruence

$$12x \equiv 15 \pmod{21}.$$

Since $\text{hcf}(12, 21) = 3$, and 3 divides 15, the congruence has three solutions modulo 21.

Cancellation of the common 3 reduces the congruence to

$$4x \equiv 5 \pmod{7}$$

which has a unique solution modulo 7, since $\text{hcf}(4, 7) = 1$. That solution is

$$x \equiv 3 \pmod{7}$$

as can be seen from $4 \times 3 \equiv 5 \pmod{7}$. The argument in the proof of part (c) then supplies the three solutions modulo 21 as

$$\begin{aligned}x &\equiv 3 \pmod{21}, \\x &\equiv 3 + 7 = 10 \pmod{21} \text{ and} \\x &\equiv 3 + 2 \times 7 = 17 \pmod{21}.\end{aligned}$$

Exercise 3.2

How many solutions does each of the following linear congruences have?

- (a) $5x \equiv 13 \pmod{10}$
- (b) $5x \equiv 10 \pmod{13}$
- (c) $10x \equiv 5 \pmod{30}$
- (d) $27x \equiv 318 \pmod{24}$

3.3 Solving linear congruences

It is nice to have a theoretical result telling us that solutions exist, but it is more important to be able to find those solutions.

Worked Exercise 3.5

Solve the linear congruence $30x \equiv 15 \pmod{33}$.

Solution

As $\text{hcf}(30, 33) = 3$ and 3 divides 15, Theorem 3.4 guarantees that the congruence has three solutions modulo 33. Failing all else, we know that we could find these solutions by substituting for x each of the values $0, 1, 2, 3, \dots, 32$ and recording which are solutions. But this last resort can usually be avoided, and can here, as we will illustrate.

For a start we can use the cancellation laws to reduce the modulus. By the Cancellation Rule, Proposition 1.8 of this chapter, the common factor 3 in both coefficients and modulus can be cancelled to give the equivalent congruence

$$10x \equiv 5 \pmod{11}.$$

As $\text{hcf}(10, 11) = 1$ we know, by Theorem 3.4(b), that this congruence has a unique solution modulo 11.

Next we can cancel further. By the Cancellation Rule the common factor 5 in the coefficients can be cancelled, this time the modulus remaining unchanged:

$$2x \equiv 1 \pmod{11}.$$

There are a number of ways of determining the unique solution modulo 11 from here. For example, we could replace the number 1 on the right-hand side of the congruence with 12, since $1 \equiv 12 \pmod{11}$:

$$2x \equiv 12 \pmod{11}.$$

Finally, cancellation of the common factor 2 of the coefficients yields the solution:

$$x \equiv 6 \pmod{11}.$$

Alternatively we could have multiplied through the congruence $2x \equiv 1 \pmod{11}$ by 6, obtaining

$$12x \equiv 6 \pmod{11},$$

whereupon replacement of the coefficient 12 by the congruent number 1 yields the same solution

$$x \equiv 6 \pmod{11}.$$

We noted that the original congruence had three solutions modulo 33 and we have ended with a unique solution modulo 11. There is no contradiction to Theorem 3.4 here, for in the set of least positive residues modulo 33 there are three numbers, namely 6, 17 and 28, that are congruent to 6 modulo 11. Consequently the unique solution $x \equiv 6 \pmod{11}$ is equivalent to the three solutions

$$x \equiv 6, 17, 28 \pmod{33},$$

for both determine the same set of integers, namely,

$$\{\dots, -38, -27, -16, -5, 6, 17, 28, 39, 50, \dots\}.$$

So either form can be taken as the answer here. Normally, except when the context of the problem demands otherwise, we will always give the solution(s) in terms of the original modulus.

Linear congruences, like the one we have just tackled, can all be solved using the following strategy.

Strategy: to solve the linear congruence $ax \equiv b \pmod{n}$

1. Check that $\text{hcf}(a, n)$ divides b . If it does not, the congruence has no solutions. If it does:
2. Cancel any common factors of all three of a , b and n . The resulting congruence has a unique solution modulo the new modulus.

The resulting coefficients (originally a and b) can then be changed by applying the remaining steps in any order, any number of times, with the goal of reaching a congruence in which the coefficient of x is 1.

3. Cancel any common factor of the coefficients.
4. Replace either coefficient by any congruent number.
5. Multiply through the congruence by any number that is coprime to the modulus.

Step 5 needs a little clarification. To illustrate why the multiplier has to be coprime to the modulus, consider the congruence

$$7x \equiv 1 \pmod{40}.$$

If we multiply through by 6 we get

$$42x \equiv 6 \pmod{40},$$

and replacing 42 with the congruent number 2 gives

$$2x \equiv 6 \pmod{40}.$$

Plainly $x \equiv 3 \pmod{40}$ is a solution of this congruence because $2 \times 3 \equiv 6 \pmod{40}$, but it is not a solution of the original congruence because $7 \times 3 = 21 \not\equiv 1 \pmod{40}$. So somewhere along the line an extraneous solution has been introduced.

The problem arose when we multiplied through the congruence by 6, because $\text{hcf}(6, 40) > 1$. From $ax \equiv b \pmod{n}$ it is certainly true that $cax \equiv cb \pmod{n}$. But, according to Proposition 1.8, the Cancellation Rule, we can reverse the argument and draw the conclusion $ax \equiv b \pmod{n}$ from $cax \equiv cb \pmod{n}$ only when $\text{hcf}(c, n) = 1$. A solution of $cax \equiv cb \pmod{n}$ is not necessarily a solution of $ax \equiv b \pmod{n}$ unless $\text{hcf}(c, n) = 1$. Hence the coprime condition of step 5 must hold before we multiply through a congruence.

The way to become proficient at solving linear congruences is through plenty of practice at applying the above strategy. We do one more before inviting you to try your hand.

Worked Exercise 3.6

Solve $9x \equiv 15 \pmod{26}$.

Solution

As $\text{hcf}(9, 26) = 1$, step 1 tells us that $9x \equiv 15 \pmod{26}$ has a unique solution modulo 26, and step 2 is not applicable. Then

$$\begin{aligned} 9x \equiv 15 \pmod{26} &\iff 3x \equiv 5 \pmod{26}, && \text{by step 3,} \\ &\iff 27x \equiv 45 \pmod{26}, && \text{by step 5,} \\ &&& \text{multiplying by 9,} \\ &\iff x \equiv 45 \pmod{26}, && \text{by step 4,} \\ &\iff x \equiv 19 \pmod{26}, && \text{by step 4.} \end{aligned}$$

The steps that we followed in this worked exercise are certainly not unique. There are many ways of solving the congruence, but, of course, all must lead to the same conclusion.

Exercise 3.3

Solve the following linear congruences.

- (a) $28x \equiv 49 \pmod{53}$
- (b) $34x \equiv 19 \pmod{52}$
- (c) $137x \equiv 96 \pmod{19}$
- (d) $51x \equiv 8 \pmod{53}$
- (e) $18x \equiv 39 \pmod{69}$

Exercise 3.4

- (a) Solve the following linear congruences.
 - (i) $8x \equiv 12 \pmod{60}$
 - (ii) $21x \equiv 35 \pmod{47}$
 - (iii) $6x \equiv 5 \pmod{41}$
 - (iv) $5x \equiv 1 \pmod{93}$
- (b) Solve the following polynomial congruences.
 - (i) $x^3 \equiv 1 \pmod{7}$
 - (ii) $2x^2 + 4x + 5 \equiv 0 \pmod{7}$
- (c) Use congruences to solve the following linear Diophantine equations.
 - (i) $12x + 19y = 7$
 - (ii) $17x + 41y = 13$
- (d) There are 19×20 congruences of the form $ax \equiv b \pmod{20}$, since there are 19 different choices for $a \not\equiv 0 \pmod{20}$ and 20 choices for b .

For how many of these congruences does a solution exist, and for how many congruences is the solution unique?

4 Simultaneous linear congruences

Now we have seen how to solve linear congruences, we will explore the theory that allows us to solve *simultaneous* linear congruences.

4.1 The Chinese Remainder Theorem

In the first century AD the Chinese mathematician Sun Tzu posed the following problem.

Worked Exercise 4.1

Find a number that leaves remainders 2, 3 and 2 when divided by 3, 5 and 7 respectively.

Solution

In congruence notation the problem is asking for a simultaneous solution of the system

$$x \equiv 2 \pmod{3}; \quad x \equiv 3 \pmod{5}; \quad x \equiv 2 \pmod{7}.$$

We can solve this problem as follows. To satisfy the first congruence x must be of the form $3r + 2$. To satisfy the second congruence as well requires

$$3r + 2 \equiv 3 \pmod{5}, \quad \text{that is,} \quad 3r \equiv 1 \pmod{5}.$$

This has the unique solution $r \equiv 2 \pmod{5}$, that is, $r = 5s + 2$ for some integer s . Therefore

$$x = 3r + 2 = 3(5s + 2) + 2 = 15s + 8.$$

This number has to satisfy the third and final congruence:

$$15s + 8 \equiv 2 \pmod{7} \iff s + 1 \equiv 2 \pmod{7}.$$

This has the unique solution $s \equiv 1 \pmod{7}$. So $s = 7t + 1$ for some integer t and, substituting into the expression for x ,

$$x = 15(7t + 1) + 8 = 105t + 23.$$

Any integer x of this form satisfies all three congruences. The least positive solution is 23 (corresponding to $t = 0$) and the complete solution is $x \equiv 23 \pmod{105}$.

By ‘simultaneous solution’ we mean an x that satisfies *all* the congruences.

Consider now a general **system of simultaneous linear congruences** to be solved, that is, a system

$$a_1x \equiv b_1 \pmod{n_1}; a_2x \equiv b_2 \pmod{n_2}; \dots; a_rx \equiv b_r \pmod{n_r}.$$

For an integer x to be a **simultaneous solution** of the system it must be a solution of each of the r individual congruences, and consequently a necessary condition for a solution is that

$$\text{hcf}(a_i, n_i) \text{ divides } b_i, \quad \text{for each } i = 1, 2, \dots, r.$$

Assuming that this condition holds, a first step in solving the simultaneous system is to solve each individual congruence, finding its unique solution for the appropriate modulus. We can do this by applying the strategy for solving linear congruences given in the previous section, leading to congruences in which the coefficient of x is 1. So from then on we can confine attention to solving simultaneous systems of the form

$$x \equiv b_1 \pmod{n_1}; x \equiv b_2 \pmod{n_2}; \dots; x \equiv b_r \pmod{n_r}$$

as in Sun Tzu's problem.

The fact that each congruence is solvable is not sufficient on its own for the simultaneous system to have a solution. For example, consider the following system:

$$x \equiv 1 \pmod{2}; x \equiv 2 \pmod{4}.$$

No even integer satisfies the first congruence and no odd integer satisfies the second; hence the simultaneous system has *no* solutions.

Inconsistencies, such as the one illustrated here, can arise when two linear congruences have moduli that are not coprime. However, if we restrict ourselves to systems in which every pair of moduli is coprime, it turns out that simultaneous solutions always exist.

Theorem 4.2 Chinese Remainder Theorem

Let $n_1, n_2, \dots, n_r$ be natural numbers such that $\text{hcf}(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv b_1 \pmod{n_1}; x \equiv b_2 \pmod{n_2}; \dots; x \equiv b_r \pmod{n_r}$$

has a simultaneous solution that is unique modulo $n_1n_2 \cdots n_r$.

The moduli $n_1, n_2, \dots, n_r$ are said to be pairwise coprime.

Proof We prove the theorem by first constructing a solution and then showing that it is unique modulo $n_1n_2 \cdots n_r$.

Let $N = n_1n_2 \cdots n_r$ and $N_k = \frac{N}{n_k}$, for $k = 1, 2, \dots, r$. Then, since $\text{hcf}(n_i, n_k) = 1$ for each $i \neq k$, it follows that

$$\text{hcf}(N_k, n_k) = \text{hcf}(n_1n_2 \cdots n_{k-1}n_{k+1} \cdots n_r, n_k) = 1,$$

and so the linear congruence $N_kx \equiv 1 \pmod{n_k}$ has a unique solution modulo n_k . Let this solution be x_k , so $N_kx_k \equiv 1 \pmod{n_k}$.

We will show that the integer

$$x_0 = b_1 N_1 x_1 + b_2 N_2 x_2 + \cdots + b_r N_r x_r$$

satisfies each of the congruences. To achieve this we evaluate x_0 modulo n_k , for each $k = 1, 2, 3, \dots, r$.

We start by noting that, whenever $i \neq k$, since n_k divides N_i , we have $N_i \equiv 0 \pmod{n_k}$. Consequently

$$x_0 \equiv b_k N_k x_k \pmod{n_k}, \quad \text{for each } k = 1, 2, \dots, r,$$

as each of the remaining terms in the sum is congruent to 0 modulo n_k .

Finally, since x_k was found such that $N_k x_k \equiv 1 \pmod{n_k}$, we have

$$x_0 \equiv b_k \pmod{n_k}$$

as claimed.

It remains to show that the discovered solution is unique modulo the product $n_1 n_2 \cdots n_r$. To this end suppose that x' is a second simultaneous solution of the system, that is,

$$x_0 \equiv x' \equiv b_k \pmod{n_k}, \quad \text{for each } k = 1, 2, \dots, r.$$

This implies that each n_k divides $x' - x_0$, whereupon the fact that the moduli are pairwise coprime gives us by Lemma 4.11 of Chapter 1 that

$$n_1 n_2 \cdots n_r \text{ divides } x' - x_0.$$

This amounts to

$$x' \equiv x_0 \pmod{n_1 n_2 \cdots n_r}$$

exactly as required. ■

To illustrate the proof of the Chinese Remainder Theorem, we trace its steps in an example.

Worked Exercise 4.3

Solve the system of simultaneous linear congruences

$$x \equiv 5 \pmod{6}; \quad x \equiv 4 \pmod{11}; \quad x \equiv 3 \pmod{17}.$$

Solution

The given values of the variables in the proof are

$$\begin{aligned} \text{coefficients: } & b_1 = 5, \quad b_2 = 4, \quad b_3 = 3; \\ \text{moduli: } & n_1 = 6, \quad n_2 = 11, \quad n_3 = 17. \end{aligned}$$

The calculated values are

$$\begin{aligned} N &= 6 \times 11 \times 17 = 1122, \quad N_1 = 11 \times 17 = 187, \\ N_2 &= 6 \times 17 = 102, \quad N_3 = 6 \times 11 = 66. \end{aligned}$$

The values x_i are obtained by solving the linear congruences $N_i x \equiv 1 \pmod{n_i}$.

$$\begin{aligned} N_1 x \equiv 1 \pmod{n_1} &\iff 187x \equiv 1 \pmod{6} \\ &\iff x \equiv 1 \pmod{6}; \text{ so } x_1 = 1. \\ N_2 x \equiv 1 \pmod{n_2} &\iff 102x \equiv 1 \pmod{11} \\ &\iff 3x \equiv 1 \pmod{11} \\ &\iff x \equiv 4 \pmod{11}; \text{ so } x_2 = 4. \\ N_3 x \equiv 1 \pmod{n_3} &\iff 66x \equiv 1 \pmod{17} \\ &\iff -2x \equiv -16 \pmod{17} \\ &\iff x \equiv 8 \pmod{17}; \text{ so } x_3 = 8. \end{aligned}$$

Therefore

$$\begin{aligned} x_0 &= 5 \times 187 \times 1 + 4 \times 102 \times 4 + 3 \times 66 \times 8 = 4151 \\ &\equiv 785 \pmod{1122}. \end{aligned}$$

Exercise 4.1

Find the least natural number n such that 3^2 divides $2n + 3$, 4^2 divides $3n + 4$ and 5^2 divides $4n + 5$.

4.2 Solving simultaneous congruences

One situation in which a system of simultaneous linear congruences can be introduced is when confronted with the problem of solving a single linear congruence in which the modulus is large and composite. To see how this works, let n have prime decomposition $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and compare the linear congruence

$$ax \equiv b \pmod{n}$$

and the system

$$ax \equiv b \pmod{p_1^{k_1}}; ax \equiv b \pmod{p_2^{k_2}}; \dots; ax \equiv b \pmod{p_r^{k_r}}.$$

Certainly any integer x that satisfies $ax \equiv b \pmod{n}$ also satisfies each congruence in the system, because $p_i^{k_i}$ divides n for each i . On the other hand, since the p_i are pairwise coprime, repeated use of Corollary 1.7 of this chapter tells us that any solution of the simultaneous system must satisfy $ax \equiv b \pmod{n}$. So the two are equivalent.

We will solve a problem of this sort in Worked Exercise 4.4. However, in this exercise we abandon the formal approach of Worked Exercise 4.3 and Exercise 4.1, in which we traced the explicit construction of a solution as given in the proof of the Chinese Remainder Theorem. The method that we adopt here, like our solution of Sun Tzu's problem at the beginning of the section, will not require the same amount of careful arithmetic. Indeed, we often treat the Chinese Remainder Theorem as an important theoretical result that confirms the existence of solutions, but apply other methods, such as the one we are about to illustrate, to discover what those solutions are.

Worked Exercise 4.4

Solve the linear congruence $3x \equiv 5 \pmod{1001}$.

Solution

Observing that $1001 = 7 \times 11 \times 13$, we seek the simultaneous solution of

$$3x \equiv 5 \pmod{7}; \quad 3x \equiv 5 \pmod{11}; \quad 3x \equiv 5 \pmod{13}.$$

That is (having first solved each of these congruences individually),

$$x \equiv 4 \pmod{7}; \quad x \equiv 9 \pmod{11}; \quad x \equiv 6 \pmod{13}.$$

The natural numbers x that satisfy the congruence $x \equiv 6 \pmod{13}$ are

$$x = 6, 19, 32, 45, 58, 71, 84, 97, \dots$$

Now 97 is the first of these integers that is congruent to 9 modulo 11, and consequently, $x \equiv 97 \pmod{11 \times 13}$ is the unique solution of the final pair of congruences of the system. The natural numbers in this solution set are

$$x = 97, 240, 383, 526, 669, \dots$$

Now 669 is the first of these that is also congruent to 4 modulo 7, and hence is the smallest natural number satisfying all three congruences. Hence

$$x \equiv 669 \pmod{7 \times 11 \times 13}$$

is the unique solution of the congruence. This method is illustrated in Figure 4.1.

Note that the numbers satisfying one congruence also form a pattern with respect to the next congruence in the system. For instance,

$$\begin{aligned} x &= 6, 19, 32, 45, 58, 71, 84, \dots \\ &\equiv 6, 8, 10, 1, 3, 5, 7, \dots \pmod{11}. \end{aligned}$$

Examining this pattern, it is possible to see quite quickly where the solution that is congruent to 9 modulo 11 is going to fall.

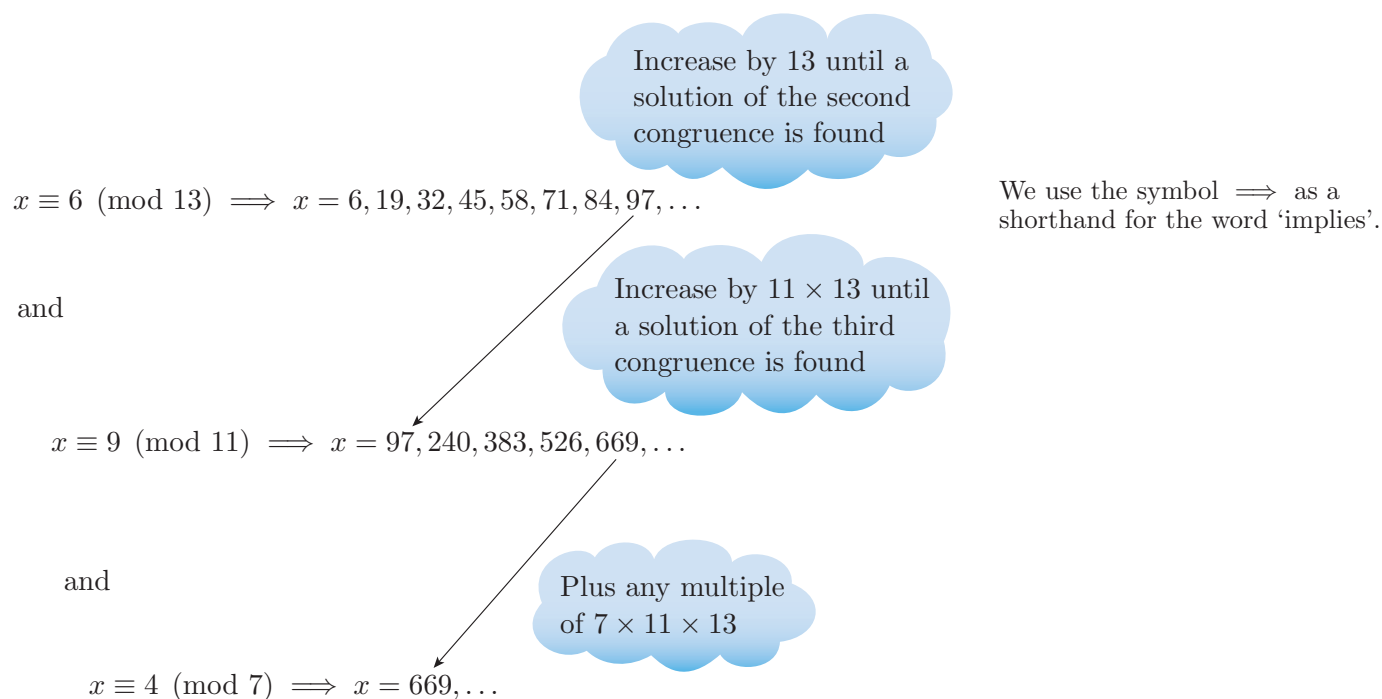


Figure 4.1 Solving simultaneous linear congruences

Exercise 4.2

Solve the linear congruence $7x \equiv 9 \pmod{165}$.

There remains one loose end to tidy up. We have seen that when a system of linear congruences has moduli that are not pairwise coprime, the system may be inconsistent and have no solutions. But this is not necessarily the case. For instance, the system

$$x \equiv 2 \pmod{6}; \quad x \equiv 5 \pmod{9}$$

involves moduli that are not pairwise coprime. However, $x = 14$ certainly satisfies both congruences, and so solutions do exist.

Theorem 4.5

The system of linear congruences

$$x \equiv b_1 \pmod{n_1}; \quad x \equiv b_2 \pmod{n_2}$$

has a simultaneous solution if, and only if, $\text{hcf}(n_1, n_2)$ divides $b_2 - b_1$. If a solution exists then it is unique modulo $\text{lcm}(n_1, n_2)$.

Proof Suppose that the integer x satisfies both

$$x \equiv b_1 \pmod{n_1} \quad \text{and} \quad x \equiv b_2 \pmod{n_2}.$$

That is, there exist integers r and s such that

$$x - b_1 = n_1 r \quad \text{and} \quad x - b_2 = n_2 s.$$

Eliminating x from this pair of equations leads to

$$b_2 - b_1 = n_1 r - n_2 s.$$

Now the right-hand side is an integer combination of n_1 and n_2 and, as such, is a multiple of $\text{hcf}(n_1, n_2)$. Thus $\text{hcf}(n_1, n_2)$ divides $b_2 - b_1$, and so this is a necessary condition for the system to have a solution.

To confirm that the condition is sufficient to guarantee a solution, we reverse the argument. Suppose that

$$b_2 - b_1 = k \text{hcf}(n_1, n_2), \quad \text{for some integer } k.$$

Now we know that there exist integers u and v such that

$$\text{hcf}(n_1, n_2) = un_1 + vn_2.$$

Elimination of $\text{hcf}(n_1, n_2)$ from this pair of equations produces

$$b_1 + kun_1 = b_2 - kvn_2.$$

Then

$$b_1 + kun_1 = b_1 + (ku)n_1 \equiv b_1 \pmod{n_1}$$

and

$$b_1 + kun_1 = b_2 - (kv)n_2 \equiv b_2 \pmod{n_2}.$$

So $b_1 + kun_1$ satisfies both congruences and confirms that simultaneous solutions do exist.

Finally, there is the question of uniqueness. Suppose that x_1 and x_2 are two solutions. That is,

$$x_1 \equiv x_2 \equiv b_1 \pmod{n_1} \quad \text{and} \quad x_1 \equiv x_2 \equiv b_2 \pmod{n_2}.$$

Theorem 1.6 of this chapter now completes the task:

$$x_1 \equiv x_2 \pmod{\text{lcm}(n_1, n_2)}. \quad \blacksquare$$

The result of Theorem 4.5 can be generalised to cover any number of congruences. A proof using mathematical induction is readily available but is omitted here as the details are somewhat tedious.

Corollary 4.6

The system of linear congruences

$$x \equiv b_1 \pmod{n_1}; \quad x \equiv b_2 \pmod{n_2}; \quad \dots; \quad x \equiv b_r \pmod{n_r}$$

has a simultaneous solution if, and only if, $\text{hcf}(n_i, n_j)$ divides $b_j - b_i$ for each pair i, j of suffixes. If a solution exists it is unique modulo $\text{lcm}(n_1, n_2, \dots, n_r)$.

Exercise 4.3

For each of the following systems of simultaneous linear congruences, decide whether or not it has solutions and, if so, solve the system.

- (a) $x \equiv 7 \pmod{12}; \quad x \equiv 11 \pmod{18}; \quad x \equiv 1 \pmod{23}$
- (b) $x \equiv 4 \pmod{12}; \quad x \equiv 10 \pmod{18}; \quad x \equiv 3 \pmod{7}$

Throughout the remainder of the topic we will continue to meet congruence problems. It may be surprising how often the task of solving linear congruences crops up in the context of deeper problems.

The final exercise in this chapter gives you some further practice at solving congruence problems.

Exercise 4.4

- (a) Solve the following system of congruences by following the steps in the proof of the Chinese Remainder Theorem.

$$x \equiv 1 \pmod{4}; \quad x \equiv 3 \pmod{5}; \quad x \equiv 0 \pmod{7}$$

- (b) Solve the following systems of congruences by any method.

(i) $2x \equiv 3 \pmod{5}; \quad 3x \equiv 4 \pmod{7}; \quad 4x \equiv 9 \pmod{11}$

(ii) $x \equiv 1 \pmod{4}; \quad x \equiv 3 \pmod{6}; \quad x \equiv 3 \pmod{9}$

- (c) Solve the following linear congruence.

$$19x \equiv 7 \pmod{2310}$$

- (d) Find the smallest natural number n such that 3^2 divides n , 4^2 divides $n + 1$ and 5^2 divides $n + 2$.

- (e) In the arithmetic progression

$$7, 18, 29, 40, 51, \dots$$

find the first three consecutive terms that are divisible by 2, 3 and 5 respectively (that is, the first of the three consecutive terms is divisible by 2, the second is divisible by 3 and the third is divisible by 5).

- (f) For which values of c does the following system of congruences have a simultaneous solution?

$$5x \equiv c \pmod{12}; \quad 7x \equiv 2 \pmod{30}$$

- (g) A band of seventeen pirates stole a sack of gold coins. On attempting to divide the spoils into equal portions, they found that four coins were left over. A brawl over who should get the extra coins followed and one pirate was killed. When the spoils were redistributed amongst the survivors, ten coins were left over. Again an argument developed and one pirate was killed. But now the spoils divided equally between the remaining pirates. What was the least number of coins that could have been stolen?

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should:

- (a) Understand the meaning of the terms ‘congruence’ and ‘residue class’, and be confident in using these to manipulate expressions in modular arithmetic.
- (b) Recognise and be able to use the connection between divisibility tests and congruence.
- (c) Be able to distinguish between distinct solutions of polynomial congruences, and apply basic methods to solve basic polynomial congruences with low modulus.
- (d) Be able to use divisibility tests, in particular those for divisibility by 9 and 11, and explain why they work.
- (e) Understand the proof of the solution of linear congruences, and be able to apply the theory to specific examples.
- (f) Recall and be able to apply the strategy to solve linear congruences, and use this to solve certain linear Diophantine equations.
- (g) Understand the statement, proof and applications of the Chinese Remainder Theorem.
- (h) Be able to use a range of techniques to solve simultaneous linear congruences.

Solutions to exercises

Solution to Exercise 1.1

- (a) False, as $3 - 29 = -26$, which is not a multiple of 8.
- (b) True, as $3 - (-29) = 32 = 4 \times 8$.
- (c) True, as $63 - 37 = 26 = 2 \times 13$.
- (d) True, as $37 - 63 = -26 = (-2) \times 13$.
- (e) True, as $63 - 63 = 0 = 0 \times 37$.
- (f) False, as $63 - 13 = 50 = 2 \times 25$, so $63 \equiv 13 \pmod{25}$.

From the definition of factors (Definition 4.3 of Chapter 1), 0 is divisible by every natural number.

Solution to Exercise 1.2

Since $a \equiv b \pmod{n}$, let k be the integer such that $a - b = kn$.

- (a) As m divides n we have $n = mr$ for some integer r . Therefore

$$a - b = kn = k(mr) = (kr)m,$$

which confirms that $a \equiv b \pmod{m}$.

- (b) Multiplying by m gives

$$\begin{aligned} ma - mb &= mkn = k(mn), & \text{confirming } ma &\equiv mb \pmod{mn}, \\ &= (mk)n, & \text{confirming } ma &\equiv mb \pmod{n}. \end{aligned}$$

- (c) Dividing by d gives

$$\frac{a}{d} - \frac{b}{d} = k\frac{n}{d}, \quad \text{in which } \frac{a}{d}, \frac{b}{d} \text{ and } \frac{n}{d} \text{ are integers.}$$

This implies that $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

- (d) Let $\text{hcf}(a, n) = d_1$ and $\text{hcf}(b, n) = d_2$. Since d_1 divides a , and d_1 divides n , it follows that d_1 divides $a - kn$; that is, d_1 divides b . But then d_1 is a common factor of b and n , and so $d_1 \leq d_2$.

On the other hand, d_2 divides b , and d_2 divides n , giving d_2 divides $b + kn$; that is, d_2 divides a . So d_2 is a common factor of a and n , and so $d_2 \leq d_1$. Hence the equality $d_1 = d_2$ follows.

- (e) Here $(a + c) - (b + c) = a - b = kn$, and so $a + c \equiv b + c \pmod{n}$.

Note that the result in part (e) is just a special, but important, case of Theorem 1.2(d) in which $d = c$.

Solution to Exercise 1.3

- (a) (i) The set of least positive residues modulo 10 is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

The set of least absolute residues modulo 10 is

$$\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}.$$

- (ii) The set of least positive residues modulo 11 is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

The set of least absolute residues modulo 11 is

$$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}.$$

- (b) (i) Replacing each of the numbers by the least positive residue to which it is congruent modulo 11 (for instance
- $-3 \equiv 8$
- ,
- $22 \equiv 0$
- , etc.), we obtain

$$\{6, 2, -3, 22, 23, -7, 7, 9, 43, -8, 16\} \equiv \{6, 2, 8, 0, 1, 4, 7, 9, 10, 3, 5\}.$$

As the latter is the set of least positive residues modulo 11, the former is a complete set of residues modulo 11.

- (ii) As $10^2 = 100 \equiv 1$ and $1^2 \equiv 1 \pmod{11}$, the eleven numbers do not form a complete set of residues. In fact only six residue classes are represented in this set, as $9^2 \equiv 2^2$, $8^2 \equiv 3^2$, $7^2 \equiv 4^2$ and $6^2 \equiv 5^2$.
- (iii) Starting from 1, each subsequent number is obtained by doubling. To avoid calculation of high powers of 2, we can write down the least positive residue for each of the numbers by systematically ‘doubling modulo 11’. The given eleven numbers are congruent, in order, to the following numbers modulo 11:

$$0, 1, 2, 4, 8, 16 \equiv 5, 10, 20 \equiv 9, 18 \equiv 7, 14 \equiv 3, 6.$$

As these numbers form the set of least positive residues modulo 11, the given set is a complete set of residues.

When there is no ambiguity over which modulus is involved we will occasionally, as in this solution, use the $\equiv$ symbol without its accompanying $(\text{mod } n)$.

Each time 11 is exceeded, the number is replaced by the least positive residue and doubling begins again.

Solution to Exercise 1.4

In $\mathbb{Z}_{10}$:

$$[6] + [8] = [6 + 8] = [14] = [4], \text{ since } 14 \equiv 4 \pmod{10}.$$

$$[6] \times [8] = [6 \times 8] = [48] = [8], \text{ since } 48 \equiv 8 \pmod{10}.$$

Allowing b to take each of the values $0, 1, 2, \dots, 9$ in turn, we find that the corresponding values of $[6] \times [b]$ are $[0], [6], [2], [8], [4], [0], [6], [2], [8]$ and $[4]$. So $[6] \times [b] = [8]$ has the two solutions $[b] = [3]$ and $[b] = [8]$.

Repeating in $\mathbb{Z}_{11}$:

$$[6] + [8] = [14] = [3], \text{ since } 14 \equiv 3 \pmod{11}.$$

$$[6] \times [8] = [48] = [4], \text{ since } 48 \equiv 4 \pmod{11}.$$

$$[6] \times [b] = [8] \text{ has the unique solution } [b] = [5].$$

Solution to Exercise 1.5

- (a) We first note that if $n \geq 7$ then 7 divides $n!$ and so $n! \equiv 0 \pmod{7}$. Therefore we have the simplification

$$1! + 2! + 3! + \cdots + 1000! \equiv 1! + 2! + 3! + \cdots + 6! \pmod{7}$$

(which removes all fear of the problem!). Now, working modulo 7, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24 \equiv 3$, $5! = 5 \times 4! \equiv 5 \times 3 \equiv 1$ and $6! = 6 \times 5! \equiv 6 \times 1 = 6$. And so,

$$1! + 2! + 3! + \cdots + 1000! \equiv 1 + 2 + 6 + 3 + 1 + 6 = 19 \equiv 5 \pmod{7},$$

and the remainder on dividing by 7 is 5.

- (b) $a^2 - 1$ is divisible by 24 precisely when $a^2 - 1 \equiv 0 \pmod{24}$ or equivalently, adding 1 to both sides and appealing to Theorem 1.2(d), when $a^2 \equiv 1 \pmod{24}$. So our task is to show that any integer a that is divisible neither by 2 nor by 3 must satisfy $a^2 \equiv 1 \pmod{24}$.

The Division Algorithm tells us that a can be written as

$$a = 24q + r, \text{ where } 0 \leq r < 24.$$

But, written in this way, a is divisible by 2 when r is even, and is divisible by 3 when r is divisible by 3. There are just eight values of r that are not divisible by either 2 or 3, namely $r = 1, 5, 7, 11, 13, 17, 19$ and 23. For a to be not divisible by either 2 or 3 it must be congruent to one of these eight values modulo 24. Thus we have, on replacing each of the last four listed values by its least absolute residue,

$$a \equiv \pm 1, \pm 5, \pm 7 \text{ or } \pm 11 \pmod{24}.$$

Now appealing to Theorem 1.2(f) gives

$$a^2 \equiv 1, 25, 49 \text{ or } 121 \pmod{24}.$$

But each of these numbers has remainder 1 when divided by 24, and the result follows.

Solution to Exercise 1.6

- (a) We wish to cancel the common factor 6. As $\text{hcf}(6, 30) = 6$, we also divide the modulus by 6:

$$6x \equiv 18 \pmod{30} \iff x \equiv 3 \pmod{5}.$$

- (b) In order to cancel the common factor 10, the modulus has to be divided by $\text{hcf}(10, 45) = 5$. So

$$20x \equiv 30 \pmod{45} \iff 2x \equiv 3 \pmod{9}.$$

- (c) The common factor 13 can be cancelled without adjustment to the modulus, since $\text{hcf}(13, 60) = 1$. So

$$52x \equiv 39 \pmod{60} \iff 4x \equiv 3 \pmod{60}.$$

Solution to Exercise 1.7

- (a) (i) Since $1997 = 7 \times 285 + 2$,
the least positive residue is 2, and
the least absolute residue is 2.
- (ii) Since $1997 = 17 \times 117 + 8$,
the least positive residue is 8, and
the least absolute residue is 8.
- (iii) Since $1997 = 101 \times 19 + 78$,
the least positive residue is 78, and
the least absolute residue is $78 - 101 = -23$.
- (b) If $k \equiv 1 \pmod{12}$ then $k = 12r + 1$, for some integer r . Hence
 $6k + 5 = 72r + 11$.
- (i) As 4 divides 72, we have $6k + 5 \equiv 11 \equiv 3 \pmod{4}$, and so 3 is the
required least positive residue.
- (ii) As 9 divides 72, we have $6k + 5 \equiv 11 \equiv 2 \pmod{9}$, and so 2 is the
required least positive residue.
- (iii) As 12 divides 72, we have $6k + 5 \equiv 11 \pmod{12}$, and so 11 is the
required least positive residue.
- (c) (i) $1^2 \equiv 6^2 \pmod{7}$ but it is not the case that $1 \equiv 6 \pmod{7}$.
- (ii) $1^2 \equiv 2^2 \pmod{3}$ and $2 \equiv 5 \pmod{3}$, but $1^5 \not\equiv 2^5 \pmod{3}$.
- (d) Let $P(n)$ be the proposition that $6^n \equiv 5n + 1 \pmod{25}$.
 $P(1)$ claims that $6 \equiv 6 \pmod{25}$, which is trivially true. We continue
by assuming that $P(k)$ is true and investigate $P(k+1)$.

$$\begin{aligned}
 6^{k+1} &= 6 \times 6^k \equiv 6 \times (5k + 1), \quad \text{by the induction hypothesis,} \\
 &\equiv 30k + 6 \pmod{25} \\
 &\equiv 5k + 6 \pmod{25} \\
 &\equiv 5(k + 1) + 1 \pmod{25},
 \end{aligned}$$

as required.

Hence the Principle of Mathematical Induction confirms that $P(n)$ is
true for all integers $n \geq 1$.

- (e) The set of n numbers will form a complete set of residues modulo n
provided no two of them are congruent modulo n . So, aiming for a
contradiction, suppose that two of the numbers are congruent
modulo n , say

$$c + ra \equiv c + sa \pmod{n}, \text{ where } 0 \leq s < r < n.$$

The definition of congruence would then give

$$n \text{ divides } (c + ra) - (c + sa).$$

That is,

$$n \text{ divides } (r - s)a.$$

But $\text{hcf}(a, n) = 1$, and so Euclid's Lemma leads to

$$n \text{ divides } r - s,$$

which is impossible since $0 < r - s < n$.

- (f) There is no unique set of steps to answer these questions. You might well have found different ways of grouping the terms from those in the solutions that follow.

- (i) As $11 \equiv 4 \pmod{7}$, we have $11^{11} \equiv 4^{11} \pmod{7}$.

Now $4^2 = 16 \equiv 2 \pmod{7}$ and so

$$11^{11} \equiv 4^{11} = (4^2)^5 \times 4 \equiv 2^5 \times 4 = 32 \times 4 \equiv 4 \times 4 \equiv 2 \pmod{7}.$$

So the remainder is 2.

- (ii) As $11^2 = 121 \equiv 2 \pmod{17}$, we have

$$11^{11} = (11^2)^5 \times 11 \equiv 2^5 \times 11 \equiv (-2) \times 11 \equiv -5 \equiv 12 \pmod{17}.$$

So the remainder is 12.

- (iii) We have

$$\begin{aligned} 11^{11} &\equiv (-8)^{11} = ((-8)^2)^5 \times (-8) \equiv 7^5 \times (-8) \pmod{19} \\ &= 7^2 \times 7^2 \times 7 \times (-8) \equiv 11 \times 11 \times (-56) \pmod{19} \\ &\equiv (-8)^2 \times 1 = 64 \equiv 7 \pmod{19}. \end{aligned}$$

So the remainder is 7.

- (g) (i) We have

$$\begin{aligned} 2^{28} &= (2^5)^5 \times 2^3 \equiv 3^5 \times 2^3 = 27 \times 9 \times 8 \pmod{29} \\ &\equiv (-2) \times 14 = -28 \equiv 1 \pmod{29}, \end{aligned}$$

which amounts to saying that 29 divides $2^{28} - 1$.

- (ii) We have

$$\begin{aligned} 3^{39} &= (3^4)^9 \times 3^3 \equiv 2^9 \times 3^3 = (8 \times 9) \times (32 \times 3) \pmod{79} \\ &\equiv (-7) \times (17) \times 2 = (-119) \times 2 \pmod{79} \\ &\equiv (-40) \times 2 = -80 \equiv -1 \pmod{79}. \end{aligned}$$

It follows that 79 divides $3^{39} + 1$.

- (h) First note that any square is congruent to either 0 or 1 modulo 3 because $0^2 \equiv 0$, $1^2 \equiv 1$ and $2^2 \equiv 1 \pmod{3}$. From this follows that $a^2 + 3b^2$ is congruent to either 0 or 1 modulo 3 since $3b^2 \equiv 0 \pmod{3}$. But $3k - 1 \equiv 2 \pmod{3}$, and so $a^2 + 3b^2$ cannot be equal to $3k - 1$ for any integer k , regardless of whether or not it is prime.
- (i) The congruences $ar \equiv b \pmod{n}$ and $cr \equiv d \pmod{n}$ tell us that there exist integers k and s such that $ar - b = kn$ and $cr - d = sn$. Substituting for b from the first of these equations and for d from the second gives

$$ad - bc = a(cr - sn) - (ar - kn)c = n(kc - as),$$

which shows that $ad \equiv bc \pmod{n}$.

Solution to Exercise 2.1

(a) (i) We have

$$N \equiv 9 + 7 + 2 + 3 \equiv 3 \pmod{9},$$

$$M \equiv 1 + 8 + 0 + 5 + 6 \equiv 2 \pmod{9},$$

$$N + M \equiv 3 + 2 \equiv 5 \pmod{9},$$

$$N - M \equiv 3 - 2 \equiv 1 \pmod{9}.$$

Hence the required remainders are 3, 2, 5 and 1 respectively.

(ii) We have

$$N \equiv 3 - 2 + 7 - 9 = -1 \equiv 10 \pmod{11},$$

$$M \equiv 6 - 5 + 0 - 8 + 1 = -6 \equiv 5 \pmod{11},$$

$$N + M \equiv 10 + 5 \equiv 4 \pmod{11},$$

$$N - M \equiv 10 - 5 \equiv 5 \pmod{11}.$$

Hence the required remainders are 10, 5, 4 and 5 respectively.

(iii) $N \times M \equiv 3 \times 2 \equiv 6 \pmod{9}$, and so the number on the right-hand side of the equation has to be congruent to 6 modulo 9.

$$1 + 7 + 5 + (?) + 5 + 8 + 4 + 8 + 8 = 46 + (?) \equiv 1 + (?) \equiv 6 \pmod{9},$$

from which it follows that the missing digit (?) can only be 5.

(b) Let $N = a_{2m-1}a_{2m-2} \dots a_2a_1a_0$ so that $M = a_0a_{2m-1}a_{2m-2} \dots a_2a_1$. Since N and M comprise the same $2m$ digits, the 9-test gives

$$N \equiv M \equiv a_0 + a_1 + a_2 + \dots + a_{2m-2} + a_{2m-1} \pmod{9},$$

and so $N - M \equiv 0 \pmod{9}$, that is, 9 divides $N - M$.

Applying the 11-test:

$$N \equiv a_0 - a_1 + a_2 - \dots + a_{2m-2} - a_{2m-1} \pmod{11}$$

whilst

$$M \equiv a_1 - a_2 + a_3 - \dots - a_{2m-2} + a_{2m-1} - a_0 \pmod{11}.$$

So $N + M \equiv 0 \pmod{11}$. That is, 11 divides $N + M$.

Finally, since $N^2 - M^2 = (N - M)(N + M)$ we have that 9 divides $N^2 - M^2$ and 11 divides $N^2 - M^2$. As $\text{hcf}(9, 11) = 1$, Corollary 1.7 allows us to conclude that 99 divides $N^2 - M^2$.

Solution to Exercise 2.2

- (a) (i) As 108 is divisible by 9, the right-hand side must be divisible by 9. Hence, adding up the digits, $4 + 0 + 0 + (?) + 8 \equiv 0 \pmod{9}$ and the only value of the digit $(?)$ that renders this possible is 6.

- (ii) Checking the calculation modulo 9,

$$1578 \times 34971 \equiv 3 \times 6 \equiv 0 \pmod{9},$$

and so the sum of the digits on the right-hand side must be divisible by 9. Thus

$$5 + 5 + 1 + 8 + (?) + 2 + 3 + 8 = 32 + (?) \equiv 5 + (?) \equiv 0 \pmod{9},$$

giving $(?) = 4$.

- (iii) The right-hand side is divisible by 11 because

$7 - 8 + 8 - 6 + 2 - 4 + 1 \equiv 0 \pmod{11}$, and so the left-hand side must be divisible by 11. Now 4473 is not divisible by 11, and so $3(?)9$ must be; that is, $9 - (?) + 3 \equiv 0 \pmod{11}$. Hence $(?) = 1$ is the only possibility.

- (b) Aiming for a contradiction, suppose that A divides B , say $B = nA$ for some integer n . Now as A comprises the digits 1 to 7, we have

$$A \equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 = 28 \equiv 1 \pmod{9}$$

and similarly $B \equiv 1 \pmod{9}$.

Since $A \equiv B \equiv 1 \pmod{9}$, the equation $B = nA$ then gives

$n \equiv 1 \pmod{9}$. Because A is not equal to B , we must have $n \geq 10$.

However, this is impossible since it forces B to have more digits than A . This contradiction shows that no such n can exist and so A does not divide B .

- (c) The key here is to note that, as M and N have the same collection of digits, $N \equiv M \pmod{9}$ or, what amounts to the same thing, $N - M \equiv 0 \pmod{9}$. But X is the sum of the digits of $N - M$ and so $X \equiv 0 \pmod{9}$. Now $N - M$ is a number with ten (or fewer) digits and so $X \leq 90$. Of all numbers not exceeding 90, the maximum sum of the digits is 17 (achieved by the number 89). X cannot be equal to 0 as that would happen if, and only if, $N = M$.

Let Y be the sum of the digits of X . Then

$$Y \equiv X \equiv 0 \pmod{9}, \quad \text{where } 0 < Y < 18.$$

Thus the only possibility is $Y = 9$.

- (d) On dividing N by 10^n , the Division Algorithm gives integers q and r such that

$$N = 10^n q + r, \quad 0 \leq r < 10^n.$$

Because of the restriction on r , it follows that r is the number made up of the last n digits of N .

Now 2^n divides 10^n and so, taking congruence modulo 2^n ,

$$N \equiv r \pmod{2^n}.$$

For example, to extract the final three digits from 1234567 we write

$$1234567 = 1234 \times 10^3 + 567.$$

Thus $N \equiv 0 \pmod{2^n}$ if, and only if, $r \equiv 0 \pmod{2^n}$; that is, 2^n divides N if, and only if, 2^n divides r , the number made up of the last n digits of N .

(e) (i) We have

$$\begin{aligned} 10^{2n} &= (10^2)^n \equiv 1^n \equiv 1 \pmod{99}, \\ 10^{2n+1} &= 10 \times 10^{2n} \equiv 10 \pmod{99}. \end{aligned}$$

(ii) Let

$$\begin{aligned} N &= a_m a_{m-1} \dots a_2 a_1 a_0 \\ &= a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \dots + a_{m-1} 10^{m-1} + a_m 10^m \\ &= (10a_1 + a_0) + 10^2(10a_3 + a_2) + 10^4(10a_5 + a_4) + \dots \end{aligned}$$

Utilising the fact that $10^{2n} \equiv 1 \pmod{99}$, we have

$$N \equiv (10a_1 + a_0) + (10a_3 + a_2) + (10a_5 + a_4) + \dots \pmod{99},$$

and the remainder on dividing by 99 can be obtained from this sum of pairs of digits.

(iii) Working modulo 101, the successive powers of 10 are

$$10^0 \equiv 1, 10^1 \equiv 10, 10^2 \equiv -1, 10^3 \equiv -10, 10^4 \equiv 1, 10^5 \equiv 10, \text{ etc.}$$

Hence

$$\begin{aligned} N &= a_m a_{m-1} \dots a_2 a_1 a_0 \\ &= a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \dots + a_{m-1} 10^{m-1} + a_m 10^m \\ &\equiv (10a_1 + a_0) - (10a_3 + a_2) + (10a_5 + a_4) - \dots \pmod{101}, \end{aligned}$$

and the remainder on dividing by 101 is obtained from this alternating sum of pairs of digits. Now

$$\begin{aligned} 62479 &\equiv 79 - 24 + 6 = 61 \pmod{101} \text{ and} \\ 9850833 &\equiv 33 - 8 + 85 - 9 = 101 \equiv 0 \pmod{101}, \end{aligned}$$

so the remainders are 61 and 0 respectively.

Solution to Exercise 3.1

(a) We evaluate $P_1(x)$ for each of the least positive residues modulo 7, namely $x = 0, 1, 2, 3, 4, 5$ and 6.

$$\begin{aligned} 0^2 + 3 \times 0 + 4 &= 4 \equiv 4 \pmod{7} \\ 1^2 + 3 \times 1 + 4 &= 8 \equiv 1 \pmod{7} \\ 2^2 + 3 \times 2 + 4 &= 14 \equiv 0 \pmod{7} \\ 3^2 + 3 \times 3 + 4 &= 22 \equiv 1 \pmod{7} \\ 4^2 + 3 \times 4 + 4 &= 32 \equiv 4 \pmod{7} \\ 5^2 + 3 \times 5 + 4 &= 44 \equiv 2 \pmod{7} \\ 6^2 + 3 \times 6 + 4 &= 58 \equiv 2 \pmod{7} \end{aligned}$$

So $P_1(x) \equiv 0 \pmod{7}$ has the one solution $x \equiv 2 \pmod{7}$.

The last term in the summation is $10^{m-1}(10a_m + a_{m-1})$ if m is odd and $10^m(0 + a_m)$ if m is even.

- (b) We need to evaluate $P_2(x)$ on a complete set of residues. This time we choose the least absolute residues modulo 5, namely $x = -2, -1, 0, 1$ and 2 .

Note that the fact that $P(a) = P(-a)$ influences the use of the least absolute residues for, as you can see, it effectively reduces the number of residues to be checked.

$$P_2(0) = -1 \equiv 4 \pmod{5}$$

$$P_2(1) = P_2(-1) = 1 - 1 \equiv 0 \pmod{5}$$

$$P_2(2) = P_2(-2) = 16 - 1 \equiv 0 \pmod{5}$$

So $P_2(x) \equiv 0 \pmod{5}$ has the four solutions $x \equiv 1, 2, -2$ and $-1 \pmod{5}$. That is, alternatively, $x \equiv 1, 2, 3$ and $4 \pmod{5}$.

Solution to Exercise 3.2

- (a) Since $\text{hcf}(5, 10) = 5$ and 5 does not divide 13, this congruence has *no* solutions.
- (b) Since $\text{hcf}(5, 13) = 1$, this congruence has a *unique* solution.
- (c) Since $\text{hcf}(10, 30) = 10$ and 10 does not divide 5, this congruence has *no* solutions.
- (d) Since $\text{hcf}(27, 24) = 3$ and 3 divides 318, this congruence has *three* solutions.

Solution to Exercise 3.3

- (a) The congruence has a unique solution modulo 53.

$$\begin{aligned} 28x &\equiv 49 \pmod{53} \iff 4x \equiv 7 \pmod{53} \quad \text{step 3} \\ &\iff 4x \equiv 60 \pmod{53} \quad \text{step 4} \\ &\iff x \equiv 15 \pmod{53} \quad \text{step 3} \end{aligned}$$

- (b) $\text{hcf}(34, 52) = 2$ and 2 does not divide 19, so the congruence has no solutions.

- (c) The congruence has a unique solution modulo 19.

$$\begin{aligned} 137x &\equiv 96 \pmod{19} \iff 4x \equiv 1 \pmod{19} \quad \text{step 4} \\ &\iff 4x \equiv 20 \pmod{19} \quad \text{step 4} \\ &\iff x \equiv 5 \pmod{19} \quad \text{step 3} \end{aligned}$$

- (d) The congruence has a unique solution modulo 53.

$$\begin{aligned} 51x &\equiv 8 \pmod{53} \iff -2x \equiv 8 \pmod{53} \quad \text{step 4} \\ &\iff 2x \equiv -8 \pmod{53} \quad \text{step 5} \\ &\iff x \equiv -4 \pmod{53} \quad \text{step 3} \\ &\iff x \equiv 49 \pmod{53} \quad \text{step 4} \end{aligned}$$

$137 \equiv 4 \pmod{19}$ and
 $96 \equiv 1 \pmod{19}$.

Rather than multiply through by -1 and then divide by 2 we could simply divide through by -2 .

- (e) As $\text{hcf}(18, 69) = 3$ and 3 divides 39, this congruence has three solutions modulo 69.

$$\begin{aligned}
 18x \equiv 39 \pmod{69} &\iff 6x \equiv 13 \pmod{23} && \text{step 2} \\
 &\iff 6x \equiv 36 \pmod{23} && \text{step 4} \\
 &\iff x \equiv 6 \pmod{23} && \text{step 3} \\
 &\iff x \equiv 6, 29, 52 \pmod{69}
 \end{aligned}$$

The final step gives the derived solution in terms of the original modulus.

We still use the equivalence symbol $\iff$ despite the different moduli, because an integer x is a solution of the previous congruence if, and only if, it is a solution of the following congruence.

Solution to Exercise 3.4

- (a) (i) $8x \equiv 12 \pmod{60} \iff 2x \equiv 3 \pmod{15}$
 $\iff 2x \equiv 18 \pmod{15}$
 $\iff x \equiv 9 \pmod{15}$
 $\iff x \equiv 9, 24, 39, 54 \pmod{60}$
- (ii) $21x \equiv 35 \pmod{47} \iff 3x \equiv 5 \pmod{47}$
 $\iff 3x \equiv -42 \pmod{47}$
 $\iff x \equiv -14 \equiv 33 \pmod{47}$
- (iii) $6x \equiv 5 \pmod{41} \iff 42x \equiv 35 \pmod{41}$
 $\iff x \equiv 35 \pmod{41}$
- (iv) $5x \equiv 1 \pmod{93} \iff 95x \equiv 19 \pmod{93}$
 $\iff 2x \equiv 112 \pmod{93}$
 $\iff x \equiv 56 \pmod{93}$

- (b) (i) Working modulo 7 gives

$$0^3 \equiv 0, 1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv 6, 4^3 \equiv 1, 5^3 \equiv 6 \text{ and } 6^3 \equiv 6.$$

Therefore the equation $x^3 \equiv 1 \pmod{7}$ has solutions $x \equiv 1, 2, 4 \pmod{7}$.

- (ii) The value of $2x^2 + 4x + 5 \pmod{7}$ for each of the seven values of x in a complete set of residues is given in the following table.

x	0	1	2	3	4	5	6
$2x^2 + 4x + 5$	5	4	0	0	4	5	3

Hence $2x^2 + 4x + 5 \equiv 0$ has the two solutions $x \equiv 2, 3 \pmod{7}$.

- (c) (i) The obvious moduli to try are 12 and 19 as each of these eliminates one of the variables.

Writing the equation as a congruence modulo 12 gives

$$19y \equiv 7 \pmod{12},$$

which on replacing 19 by the congruent number 7 simplifies to

$$y \equiv 1 \pmod{12}.$$

Substituting $y = 1$ into the original equation gives $x = -1$, and so the general solution is

$$x = -1 + 19k, \quad y = 1 - 12k, \quad k \in \mathbb{Z}.$$

- (ii) Writing the equation modulo 17 we have

$$\begin{aligned} 41y &\equiv 13 \pmod{17} \iff 7y \equiv 13 \pmod{17} \\ &\iff 35y \equiv 65 \pmod{17} \quad \text{multiplying by 5} \\ &\iff y \equiv 14 \equiv -3 \pmod{17}. \end{aligned}$$

Substituting $y = -3$ into the original equation gives $x = 8$, and hence the general solution is

$$x = 8 + 41k, \quad y = -3 - 17k, \quad k \in \mathbb{Z}.$$

- (d) Take the uniqueness first. The congruence $ax \equiv b \pmod{20}$ has a unique solution if, and only if, $\text{hcf}(a, 20) = 1$; that is, when $a = 1, 3, 7, 9, 11, 13, 17$ and 19 . For each of these eight values of a there are twenty values of b , making 160 congruences in total for which the solution is unique.

The congruence has $\text{hcf}(a, 20)$ solutions whenever $\text{hcf}(a, 20)$ divides b . So consider the possible values of $\text{hcf}(a, 20)$ in turn.

$\text{hcf}(a, 20) = 1$ leads to 160 solvable congruences, as already seen.

$\text{hcf}(a, 20) = 2$ when $a = 2, 6, 14$ and 18 . For each of these four values of a the congruence is solvable provided b takes one of the ten even values $0, 2, 4, 6, 8, 10, 12, 14, 16$ or 18 . Hence there are 40 congruences with solutions.

$\text{hcf}(a, 20) = 4$ when $a = 4, 8, 12$ and 16 . For each of these four values of a the congruence has solutions when b takes one of the five values $0, 4, 8, 12$ or 16 , making 20 congruences in all.

$\text{hcf}(a, 20) = 5$ when $a = 5$ or 15 . For each of these two values of a the congruence has solutions if b takes one of the values $0, 5, 10$ or 15 , making 8 congruences in all.

$\text{hcf}(a, 20) = 10$ when $a = 10$. In this case the congruence is solvable when $b = 0$ or 10 , making 2 congruences in all.

Altogether there are 230 congruences that have solutions.

You might like to compare this approach with that used in Subsection 5.2 of Chapter 1.

Solution to Exercise 4.1

Expressed in terms of congruence, the three conditions to be satisfied are

$$2n + 3 \equiv 0 \pmod{9}; \quad 3n + 4 \equiv 0 \pmod{16}; \quad 4n + 5 \equiv 0 \pmod{25}.$$

Solving these individually gives the equivalent system

$$n \equiv 3 \pmod{9}; \quad n \equiv 4 \pmod{16}; \quad n \equiv 5 \pmod{25},$$

as, for example,

$$\begin{aligned} 2n + 3 \equiv 0 \pmod{9} &\iff 2n \equiv -3 \pmod{9} \iff 2n \equiv 6 \pmod{9} \\ &\iff n \equiv 3 \pmod{9}. \end{aligned}$$

The variables in the proof of the Chinese Remainder Theorem are

$$b_1 = 3, \quad b_2 = 4, \quad b_3 = 5, \quad n_1 = 9, \quad n_2 = 16, \quad n_3 = 25, \quad N = 3600, \\ N_1 = 400, \quad N_2 = 225, \quad N_3 = 144.$$

$$\begin{aligned} N_1x = 400x \equiv 1 \pmod{9} &\iff 4x \equiv 1 \pmod{9} \\ &\iff x \equiv 7 \pmod{9}, \text{ so } x_1 = 7. \\ N_2x = 225x \equiv 1 \pmod{16} &\iff x \equiv 1 \pmod{16}, \text{ so } x_2 = 1. \\ N_3x = 144x \equiv 1 \pmod{25} &\iff 19x \equiv 1 \equiv 76 \pmod{25} \\ &\iff x \equiv 4 \pmod{25}, \text{ so } x_3 = 4. \end{aligned}$$

Therefore

$$x_0 = 3 \times 400 \times 7 + 4 \times 225 \times 1 + 5 \times 144 \times 4 = 12\,180 \equiv 1380 \pmod{3600}$$

and the least positive solution is $n = 1380$.

Solution to Exercise 4.2

As $165 = 3 \times 5 \times 11$, we begin by solving the linear congruence to each of the moduli 3, 5 and 11.

$$\begin{aligned} 7x \equiv 9 \pmod{3} &\iff x \equiv 0 \pmod{3} \\ 7x \equiv 9 \pmod{5} &\iff x \equiv 2 \pmod{5} \\ 7x \equiv 9 \pmod{11} &\iff x \equiv 6 \pmod{11} \end{aligned}$$

Our task is now to solve the three congruences on the right-hand side simultaneously.

$$x \equiv 6 \pmod{11} \implies x = 6, 17, \dots,$$

increasing in steps of 11 until we reach a solution of the second congruence.

$$x \equiv 2 \pmod{5} \implies x = 17, 72, \dots,$$

increasing in steps of $11 \times 5 = 55$ until we reach a solution of the remaining congruence.

$$x \equiv 0 \pmod{3} \implies x \equiv 72 \pmod{11 \times 5 \times 3}.$$

Hence

$$x \equiv 72 \pmod{165}$$

is the unique solution of the congruence.

Solution to Exercise 4.3

(a) This system has no solutions since $\text{hcf}(12, 18) = 6$ and 6 does not divide $11 - 7 = 4$.

(b) This system has solutions since $\text{hcf}(12, 18)$ divides $10 - 4$, $\text{hcf}(7, 12) = 1$ (which divides all integers) and $\text{hcf}(7, 18) = 1$.

$$x \equiv 10 \pmod{18} \implies x = 10, 28, \dots,$$

$$x \equiv 4 \pmod{12} \implies x = 28, 64, 100, 136, \dots,$$

increasing in steps of $\text{lcm}(12, 18) = 36$,

$$x \equiv 3 \pmod{7} \implies x \equiv 136, 388, 640, \dots,$$

increasing in steps of $7 \times 36 = 252$.

The solution $x \equiv 136 \pmod{252}$ is unique.

Solution to Exercise 4.4

(a) Following the proof of the Chinese Remainder Theorem, the variables are $n_1 = 4$, $n_2 = 5$, $n_3 = 7$, $N = 4 \times 5 \times 7 = 140$, $N_1 = 35$, $N_2 = 28$, $N_3 = 20$, $b_1 = 1$, $b_2 = 3$, $b_3 = 0$.

$$N_1 x_1 \equiv 1 \pmod{n_1} \iff 35x_1 \equiv 1 \pmod{4}$$

$$\iff 3x_1 \equiv 1 \pmod{4}, \text{ so } x_1 = 3.$$

$$N_2 x_2 \equiv 1 \pmod{n_2} \iff 28x_2 \equiv 1 \pmod{5}$$

$$\iff 3x_2 \equiv 1 \pmod{5}, \text{ so } x_2 = 2.$$

$$N_3 x_3 \equiv 1 \pmod{n_3} \iff 20x_3 \equiv 1 \pmod{7}$$

$$\iff -1x_3 \equiv 1 \pmod{7}, \text{ so } x_3 = 6.$$

The solution is

$$x_0 \equiv 1 \times 35 \times 3 + 3 \times 28 \times 2 + 0 \times 20 \times 6 = 273 \equiv 133 \pmod{140}.$$

The smallest natural number solution is 133.

(b) (i) We first solve the three congruences individually.

$$2x \equiv 3 \pmod{5} \iff x \equiv 4 \pmod{5}$$

$$3x \equiv 4 \pmod{7} \iff x \equiv 6 \pmod{7}$$

$$4x \equiv 9 \pmod{11} \iff x \equiv 5 \pmod{11}$$

Now,

$$x \equiv 5 \pmod{11} \implies x = 5, 16, 27, \dots,$$

increasing by 11 to a solution of the second congruence,

$$x \equiv 6 \pmod{7} \implies x = 27, 104, \dots,$$

increasing by $11 \times 7 = 77$ to a solution of the
congruence remaining,

and

$$x \equiv 4 \pmod{5} \implies x \equiv 104 \pmod{385}.$$

- (ii) As the moduli are not pairwise coprime, a little more care must be taken with this one.

$x \equiv 1 \pmod{4}$ and $x \equiv 3 \pmod{6}$ have a unique simultaneous solution modulo 12 (the least common multiple of 4 and 6), since $\text{hcf}(4, 6) = 2$ divides the difference $3 - 1$. By inspection this solution is $x \equiv 9 \pmod{12}$.

$x \equiv 9 \pmod{12}$ and $x \equiv 3 \pmod{9}$ have a unique simultaneous solution modulo 36 (the least common multiple of 12 and 9), since $\text{hcf}(12, 9) = 3$ divides the difference $9 - 3$.

$$x \equiv 9 \pmod{12} \implies x = 9, 21, \dots,$$

and

$$x \equiv 3 \pmod{9} \implies x \equiv 21 \pmod{36}.$$

- (c) $2310 = 2 \times 3 \times 5 \times 7 \times 11$ and so we require the simultaneous solution of the system

$$19x \equiv 7 \pmod{2}; \quad 19x \equiv 7 \pmod{3}; \quad 19x \equiv 7 \pmod{5};$$

$$19x \equiv 7 \pmod{7}; \quad 19x \equiv 7 \pmod{11}.$$

Solving these individually gives the equivalent system

$$x \equiv 1 \pmod{2}; \quad x \equiv 1 \pmod{3}; \quad x \equiv 3 \pmod{5};$$

$$x \equiv 0 \pmod{7}; \quad x \equiv 5 \pmod{11}.$$

Now

$$x \equiv 1 \pmod{2} \implies x = 1, \dots, \quad \text{increasing in steps of 2,}$$

$$x \equiv 1 \pmod{3} \implies x = 1, 7, 13, \dots, \quad \text{increasing in steps of 6,}$$

$$x \equiv 3 \pmod{5} \implies x = 13, 43, 73, 103, 133, \dots, \quad \text{increasing in steps of 30,}$$

$$x \equiv 0 \pmod{7} \implies x = 133, 343, 553, 763, 973, \dots, \quad \text{increasing in steps of 210.}$$

The order in which the individual congruences are incorporated does not matter. We have usually started with the one with largest modulus, but here we have chosen the opposite order.

Finally,

$$x \equiv 5 \pmod{11} \implies x \equiv 973 \pmod{2310}.$$

- (d) Translated into a problem in simultaneous congruences, we have to solve the system

$$n \equiv 0 \pmod{9}; \quad n \equiv 15 \pmod{16}; \quad n \equiv 23 \pmod{25}.$$

Now

$$n \equiv 23 \pmod{25} \implies n = 23, 48, 73, 98, 123, 148, 173, 198, 223, \dots, \quad \text{increasing in steps of 25,}$$

$$n \equiv 15 \pmod{16} \implies n = 223, 623, 1023, 1423, 1823, 2223, \dots, \quad \text{increasing in steps of } 16 \times 25 = 400.$$

Finally

$$n \equiv 0 \pmod{9} \implies n \equiv 2223 \pmod{3600}.$$

- (e) The arithmetic progression comprises numbers of the form $11k + 7$, and so three consecutive terms of the sequence are $11n + 7$, $11n + 18$ and $11n + 29$. Our task is therefore to solve, for n , the system of linear congruences

$$11n + 7 \equiv 0 \pmod{2}; \quad 11n + 18 \equiv 0 \pmod{3}; \quad 11n + 29 \equiv 0 \pmod{5},$$

which, after simplification, becomes

$$n \equiv 1 \pmod{2}; \quad n \equiv 0 \pmod{3}; \quad n \equiv 1 \pmod{5}.$$

The first and third of these congruences require that $n \equiv 1 \pmod{10}$, so

$$n = 1, 11, 21, \dots$$

The first number in this sequence to satisfy the remaining congruence, $n \equiv 0 \pmod{3}$, is $n = 21$. The three numbers in the arithmetic sequence are therefore 238, 249 and 260.

- (f) To be in a position to apply Theorem 4.5 we must first solve each individual congruence.

$$5x \equiv c \pmod{12} \iff 25x \equiv 5c \pmod{12} \iff x \equiv 5c \pmod{12}$$

$$7x \equiv 2 \pmod{30} \iff 7x \equiv -28 \pmod{30} \iff x \equiv -4 \equiv 26 \pmod{30}$$

The system has solutions when $\text{hcf}(12, 30)$ divides $26 - 5c$; that is, when 6 divides $26 - 5c$.

$$5c \equiv 26 \pmod{6} \iff 5c \equiv 20 \pmod{6} \iff c \equiv 4 \pmod{6}$$

So the system has a simultaneous solution when $c \equiv 4 \pmod{6}$.

- (g) The number of gold coins n satisfies each of the congruences

$$n \equiv 4 \pmod{17}; \quad n \equiv 10 \pmod{16}; \quad n \equiv 0 \pmod{15}.$$

Now

$$n \equiv 4 \pmod{17} \implies n = 4, 21, 38, 55, 72, 89, 106, \dots,$$

$$n \equiv 10 \pmod{16} \implies n = 106, 378, 650, 922, 1194, 1466, 1738, 2010, \dots,$$

increasing in steps of $16 \times 17 = 272$,

and

$$n \equiv 0 \pmod{15} \implies n \equiv 2010 \pmod{15 \times 16 \times 17}.$$

The least possible number of coins is 2010.

Chapter 4

Fermat's and Wilson's Theorems

Introduction

One way to investigate problems in number theory is to look at special cases of the problem and to draw general conclusions from the empirical evidence accumulated. You have already seen instances, and you will see many more, of dangers in this approach when seemingly clear patterns of behaviour can go unexpectedly wrong. Consider the numbers $2^n - 2$, for positive integers n . Investigation of the prime decompositions of these numbers would yield that $2^2 - 2$ is divisible by 2, $2^3 - 2$ is divisible by 3, $2^5 - 2$ is divisible by 5 and $2^7 - 2$ is divisible by 7. On the other hand, taking composite exponents, $2^4 - 2$ is not divisible by 4 and $2^6 - 2$ is not divisible by 6. It is beginning to look as if $2^n - 2$ is divisible by n when n is prime but not when it is composite. Trying more and more values of n , we find that $2^{17} - 2$ is divisible by 17, $2^{18} - 2$ is not divisible by 18, $2^{19} - 2$ is divisible by 19, and this no doubt fortifies our faith in the truth of this result. But no matter how much numerical evidence is gathered, we cannot be sure that the pattern really does persist until we have a general proof.

For many hundreds of years, mathematicians believed the result that $2^p - 2$ is divisible by p if, and only if, p is prime. They had good evidence to support their conjecture, but not a proof. It was 1819 before a counter-example was discovered: $341 = 11 \times 31$ is not prime but $2^{341} - 2$ is divisible by 341.

In the seventeenth century, Fermat showed interest in these numbers and he extended his researches beyond just looking at powers of 2. His interest was captured by numbers $a^p - a$ for any integer a , and he succeeded in proving that if p is prime then $a^p - a$ is divisible by p . He offered no conclusions when the exponent is composite.

You can learn more about Fermat's life in the *History Reader* for this topic.

In his book *Men of Mathematics* (1937, Pelican), E.T. Bell writes:

It is difficult if not impossible to state why some theorems in arithmetic are considered 'important' while others, equally difficult to prove, are dubbed trivial. One criterion, although not necessarily conclusive, is that the theorem should be of use in other fields of mathematics. Another is that it should suggest researches in arithmetic or in mathematics generally, and a third that it should be in some respect universal. Fermat's Theorem satisfies all of these somewhat arbitrary demands: it is of indispensable use in many departments of mathematics, including the theory of groups, which in turn is at the root of the theory of algebraic equations; it has suggested many investigations, of which the entire subject of primitive roots may be recalled to mathematical readers as an important instance; and finally it is universal in that it states a property of *all* prime numbers – such statements are extremely difficult to find and very few are known.

When, in the first section of this chapter, we meet Fermat's Theorem, which tends to be known as Fermat's Little Theorem to distinguish it from the infamous Fermat's Last Theorem (which we will meet again in Book C, Chapter 12), it may not appear to be anything remarkable. Yet as the chapter unfolds we will show many applications of the theorem, and in particular we will capitalise on its immense potential in assisting in calculations involving large numbers. Deservedly it is considered to be a cornerstone in the development of number theory.

The role of Fermat's Theorem in solving certain problems will lead us into the subject of primitive roots (referred to in the extract from Bell above). We will pursue these ideas more comprehensively in Book C, Chapter 9, but here we use them to explain the periodic behaviour of the decimal expansions of fractions.

This chapter also introduces a second important result, Wilson's Theorem, which is similar in nature to Fermat's Little Theorem although it is not connected in any way. This theorem asserts that if p is prime then $(p-1)! \equiv -1 \pmod{p}$. Wilson's Theorem shares with Fermat's Little Theorem the feature that both are concerned with properties of *all* prime numbers. What is more, they have another rare feature in common: for both there is a relatively simple general proof available!

The statements of both Fermat's and Wilson's Theorems are implications, that is, they are of the form *if A holds then B holds*. For such statements it is natural to ask about the converse: *if B holds then A holds*. The converse of Wilson's Theorem, which states that for $p > 1$, if $(p-1)! \equiv -1 \pmod{p}$ then p is prime, will be seen to be true. On the other hand, the converse of Fermat's Little Theorem will be seen to be false. It is not true that if, for all integers a , we have that $a^p - a$ is divisible by p , then p must be prime.

Chapter guide

This chapter consists of five sections, the first and third of which, on Fermat's Little Theorem and Wilson's Theorem, are slightly shorter than the second and fourth. Section 2 applies Fermat's Little Theorem to explore properties of decimal representation, while Section 4 explores the notion of congruence applied to polynomials. The fifth section is a brief, non-assessed section on two combinatorial problems that, respectively, illustrate Fermat's Little Theorem and Wilson's Theorem.

1 Fermat's Little Theorem

This first section states and proves Fermat's Little Theorem, and explores why and when the converse statement does not hold.

1.1 Statement and proof of Fermat's Little Theorem

Figure 1.1 shows the values of successive powers of an integer a modulo each of the primes $p = 3, 5$ and 7 , where a ranges over $1, \dots, p-1$.

mod 3	mod 5	mod 7
a	a	a
a^2	a^2	a^2
	a^3	a^3
	a^4	a^4
		a^5
		a^6

Figure 1.1 Powers modulo a prime

There are some interesting patterns beginning to emerge from these tables. Notice how some power in each column is congruent to 1, and thereafter the powers ‘cycle’. For instance, if we continue to determine more and more powers of 4 modulo 7 then we get the sequence

$$4, 2, 1, 4, 2, 1, 4, 2, 1, 4, 2, 1, \dots,$$

with the cycle 4, 2, 1 of length 3.

The powers of 5 modulo 7 give the sequence

$$5, 4, 6, 2, 3, 1, 5, 4, 6, 2, 3, 1, \dots,$$

with a cycle 5, 4, 6, 2, 3, 1 of length 6.

In particular, notice how the last listed row of each table consists entirely of 1s. That is, for these three prime moduli, $a^{p-1} \equiv 1 \pmod{p}$ for each $a \not\equiv 0 \pmod{p}$. The result illustrated here holds generally for any prime p , and was first formulated by Fermat. This result may look slightly different from the claim in the introduction that, for all integers a , $a^p - a$ is divisible by p , but you will shortly see that they are indeed the same.

Theorem 1.1 *Fermat's Little Theorem*

If p is a prime and a is any integer with $\text{hcf}(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

The condition $\text{hcf}(a, p) = 1$ is equivalent to each of $a \not\equiv 0 \pmod{p}$ and ‘ p does not divide a ’. Depending on the application we will use the most appropriate form.

Proof Consider the set of $p - 1$ integers

$$\{a, 2a, 3a, \dots, (p - 1)a\}.$$

None of these numbers is congruent to 0 modulo p , for if $ra \equiv 0 \pmod{p}$, Euclid's Lemma gives $r \equiv 0 \pmod{p}$ or $a \equiv 0 \pmod{p}$, neither of which is the case here. What is more, no two of these numbers are congruent to each other modulo p , for if we had

$$ra \equiv sa \pmod{p}, \text{ where } 1 \leq r \leq p - 1 \text{ and } 1 \leq s \leq p - 1,$$

then cancellation of the a , which we can do since $\text{hcf}(a, p) = 1$, gives $r \equiv s \pmod{p}$ and so $r = s$. It follows that these $p - 1$ numbers are congruent, in some order, to the numbers in the set

$$\{1, 2, 3, \dots, p - 1\}$$

consisting of the least positive residues of p , excluding zero.

So, by multiplying all the numbers in each set together, we get

$$a \times 2a \times 3a \times \dots \times (p - 1)a \equiv 1 \times 2 \times 3 \times \dots \times (p - 1) \pmod{p},$$

which gives

$$a^{p-1} \times (p - 1)! \equiv (p - 1)! \pmod{p}.$$

Since p does not divide $(p - 1)!$ the latter can be cancelled throughout the congruence, leaving $a^{p-1} \equiv 1 \pmod{p}$, as required. ■

It is certainly not true that $a^{p-1} \equiv 1 \pmod{p}$ when $a \equiv 0 \pmod{p}$, for $0^{p-1} \equiv 0 \pmod{p}$. However Fermat's Little Theorem, which we will refer to also in the abbreviated form FLT, can be expressed in an alternative way that includes the case $a \equiv 0 \pmod{p}$, as follows.

Fermat's Little Theorem, an alternative formulation

If p is a prime and a is any integer,

$$a^p \equiv a \pmod{p}.$$

Exercise 1.1

Prove that the two formulations of FLT are equivalent. That is, prove that for prime p :

- (a) if $a^p \equiv a \pmod{p}$ for all integers a , then $a^{p-1} \equiv 1 \pmod{p}$ for all $a \not\equiv 0 \pmod{p}$
- (b) if $a^{p-1} \equiv 1 \pmod{p}$ for all $a \not\equiv 0 \pmod{p}$, then $a^p \equiv a \pmod{p}$ for all integers a .

FLT has applications in many areas, as you will see. But it really comes into its own in assisting with complex calculations, as in the following worked exercise.

Worked Exercise 1.2

(a) What is the remainder when 7^{40} is divided by 17?

(b) Show that, for any odd prime p ,

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \text{ is divisible by } p.$$

Solution

(a) FLT tells us that $7^{16} \equiv 1 \pmod{17}$. Therefore, breaking the power 40 down in an appropriate way,

$$7^{40} = (7^{16})^2 \times 7^8 \equiv 1^2 \times 7^8 \equiv 7^8 \pmod{17}.$$

Now $7^2 = 49 \equiv -2 \pmod{17}$, and so

$$7^{40} \equiv 7^8 \equiv (7^2)^4 \equiv (-2)^4 \equiv 16 \pmod{17},$$

and the remainder on dividing 7^{40} by 17 is 16.

(b) By FLT, $a^p \equiv a \pmod{p}$ for all integers a . Therefore

$$\begin{aligned} 1^p + 2^p + 3^p + \cdots + (p-1)^p &\equiv 1 + 2 + 3 + \cdots + (p-1) \pmod{p} \\ &\equiv \frac{p(p-1)}{2} \pmod{p}, \quad \text{sum of an arithmetic progression} \\ &\equiv 0 \pmod{p}, \quad \text{since } \frac{p-1}{2} \text{ is an integer when } p \text{ is odd.} \end{aligned}$$

So p divides $1^p + 2^p + 3^p + \cdots + (p-1)^p$ for all odd primes p .

Exercise 1.2

(a) Find the remainder when:

(i) 5^{20} is divided by 7

(ii) 37^{37} is divided by 17.

(b) Let p be a prime and $\text{hcf}(a, p) = 1$. Use FLT to verify that

$x \equiv a^{p-2}b \pmod{p}$ is a solution of the linear congruence

$ax \equiv b \pmod{p}$. Hence solve $5x \equiv 18 \pmod{19}$.

1.2 Pseudoprimes

The converse of the alternative formulation of FLT fails to hold. That is, if $a^n \equiv a \pmod{n}$ for every integer a , it does not follow that n is prime. But counter-examples to this converse are not so easy to find. Concentration on the case $a = 2$ has historical interest. For a very long time it was thought n had to be prime for $2^n - 2$ to be divisible by n , and this was used as a test for the primality of n . Let us first put an end to that conjecture.

341 is not a counter-example to the converse of FLT since it is not true that $a^{341} \equiv a \pmod{341}$ for *all* integers a . For example, $3^{341} \equiv 168 \pmod{341}$.

Worked Exercise 1.3

Show that $2^{341} \equiv 2 \pmod{341}$.

Solution

We will show that $2^{340} \equiv 1 \pmod{341}$, from which the result follows on multiplying through by 2.

Notice that $341 = 11 \times 31$, so our line of attack will be to determine first the values of $2^{340} \pmod{11}$ and $2^{340} \pmod{31}$. As 11 and 31 are primes, we can call on FLT; this tells us that $2^{10} \equiv 1 \pmod{11}$ and that $2^{30} \equiv 1 \pmod{31}$. Working modulo 11:

$$2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}.$$

Working modulo 31:

$$2^{340} = (2^{30})^{11} \times (2^{10}) \equiv 1^{11} \times 2^5 \times 2^5 \equiv 1 \times 1 \times 1 \equiv 1 \pmod{31}.$$

As 11 and 31 are coprime we can appeal to Theorem 1.6 of Chapter 3 to conclude, from the above two congruences, that

$$2^{340} \equiv 1 \pmod{341}.$$

Pseudoprimes are sometimes called Poulet numbers, after the French mathematician who, in 1926, computed them all up to 5×10^7 .

Composite integers n with the property that n divides $2^n - 2$ are called **pseudoprimes**. They do not have to be odd numbers; the two smallest even pseudoprimes are 161 038 and 215 326. There are infinitely many pseudoprimes, although they appear to be much sparser than the primes themselves. For example, of the numbers up to 2×10^{10} , it has been shown that 882 206 716 are primes but only 19 865 are pseudoprimes. The smallest pseudoprime, discovered in 1819, is 341. The next, discovered in 1912, furnishes us with the first counter-example to the converse of FLT.

Worked Exercise 1.4

Show that $a^{561} \equiv a \pmod{561}$ for every integer a .

Solution

First, we factorise 561 as $561 = 3 \times 11 \times 17$. We will determine the value of a^{561} modulo each of 3, 11 and 17, using FLT. For any integer a ,

$$a^3 \equiv a \pmod{3}, \quad a^{11} \equiv a \pmod{11} \quad \text{and} \quad a^{17} \equiv a \pmod{17}.$$

Working modulo 3:

$$\begin{aligned} a^{561} &= (a^3)^{187} \equiv a^{187} = (a^3)^{62} \times a \equiv a^{62} \times a = a^{63} = (a^3)^{21} \equiv a^{21} \\ &= (a^3)^7 \equiv a^7 = (a^3)^2 \times a \equiv a^2 \times a = a^3 \equiv a \pmod{3}. \end{aligned}$$

Working modulo 11:

$$a^{561} = (a^{11})^{51} \equiv a^{51} = (a^{11})^4 \times a^7 \equiv a^4 \times a^7 = a^{11} \equiv a \pmod{11}.$$

Working modulo 17:

$$a^{561} = (a^{17})^{33} \equiv a^{33} = a^{17} \times a^{16} \equiv a \times a^{16} = a^{17} \equiv a \pmod{17}.$$

Theorem 1.6 of Chapter 3 now gives $a^{561} \equiv a \pmod{561}$ for all integers a . So 561 is a counter-example to the converse of FLT.

It was proved, in 1994, that there are in fact infinitely many numbers that provide a counter-example to the converse of FLT. Such numbers are called **Carmichael numbers**.

Having two seemingly different formulations of FLT requires us to decide which one to use in a given situation. When confronted with a result about *all* integers a , as in Worked Exercise 1.4, you must use $a^p \equiv a \pmod{p}$, to ensure that the argument caters for the case $a \equiv 0 \pmod{p}$. On the other hand, when dealing with a result concerning integers a for which $a \not\equiv 0 \pmod{p}$, as in Worked Exercise 1.3, although $a^p \equiv a \pmod{p}$ still applies, the alternative congruence $a^{p-1} \equiv 1 \pmod{p}$ invariably leads to simpler computations.

Exercise 1.3

- Prove that 168 divides $a^6 - 1$, where a is any integer for which $\text{hcf}(a, 42) = 1$.
- For any integer a , show that a^5 and a have the same units digit. Deduce that a^{100} has the same units digit as a^4 .

Exercise 1.4

- Find the least positive residue modulo 13 of 5^{12} , 5^{14} and 1996^{14} .
- Use FLT to show that:
 - $3^{50} + 5^{50}$ is divisible by 17
 - $2^{100} + 3^{100}$ is divisible by 97.

- (c) What is the remainder when 7^{154} is divided by 155?
Hint: $155 = 5 \times 31$.
- (d) Show that $a^7 \equiv a \pmod{42}$ for all integers a .
- (e) If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
- (f) Show that $(p-1)2^{p-1} + 1$ and $(p-2)2^{p-2} + 1$ are each divisible by the odd prime p . Is it true that $(p-3)2^{p-3} + 1$ is necessarily divisible by the odd prime p ?

2 Representation of fractions by decimals

We now use Fermat's Little Theorem to explore some properties of decimal representations.

2.1 Terminating and cycling decimals

When reciprocals of integers are written out as decimals, a variety of patterns emerge. A few reciprocals are shown in Table 2.1.

Table 2.1 Decimal representation of the reciprocals of 2 to 13

Reciprocal	Decimal representation
$\frac{1}{2}$	0.5
$\frac{1}{3}$	$0.333\dots = 0.\langle 3 \rangle$
$\frac{1}{4}$	0.25
$\frac{1}{5}$	0.2
$\frac{1}{6}$	$0.1666\dots = 0.1\langle 6 \rangle$
$\frac{1}{7}$	$0.142857142857142857\dots = 0.\langle 142857 \rangle$
$\frac{1}{8}$	0.125
$\frac{1}{9}$	$0.111\dots = 0.\langle 1 \rangle$
$\frac{1}{10}$	0.1
$\frac{1}{11}$	$0.090909\dots = 0.\langle 09 \rangle$
$\frac{1}{12}$	$0.08333\dots = 0.08\langle 3 \rangle$
$\frac{1}{13}$	$0.076923076923076923\dots = 0.\langle 076923 \rangle$

The 'angle bracket' notation is used to indicate that the string of digits in the brackets repeats indefinitely.

We observe that some of the decimals terminate while others go on forever. All the non-terminating ones have a **cycle** that is repeated indefinitely, such as the cycle $\langle 142857 \rangle$ of length 6 in $\frac{1}{7}$ and the cycle $\langle 09 \rangle$ of length 2 in $\frac{1}{11}$. In some of the decimals (for example $\frac{1}{3}$ and $\frac{1}{7}$) there is just the repeating cycle, while in others (for example $\frac{1}{6}$ and $\frac{1}{12}$) the cycle is preceded by some dissimilar digits. Can we explain these differences?

The **length of a cycle** is the number of digits forming the cycle.

To determine the decimal of $\frac{1}{7}$ by hand you might well proceed by long division, as illustrated on the left of Figure 2.1. To remind you of how long division works, at the boxed stage, 20 is divided by 7 giving a quotient of 2 and a remainder of 6. The remainder is then multiplied by 10 and the process continues by dividing 60 by 7. On the right we have presented the same set of calculations expressed in terms of the division algorithm.

Notice that the zero quotient in the first equation just gives the zero before the decimal point.

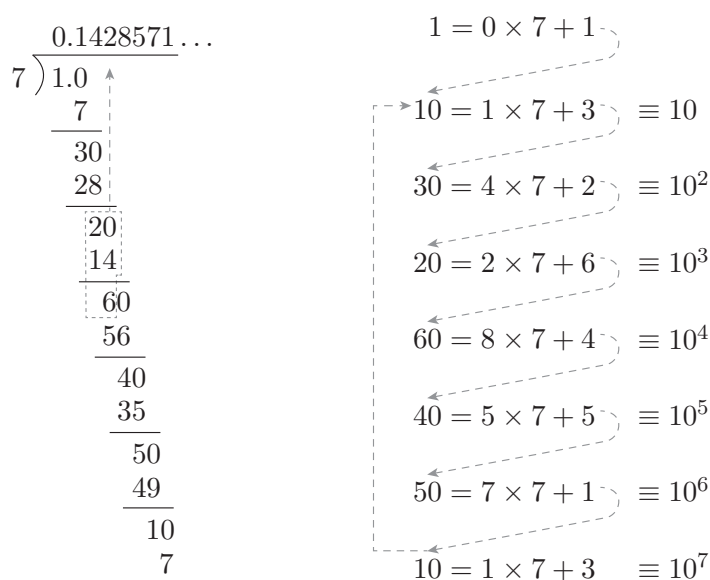


Figure 2.1 The decimal of $\frac{1}{7}$ by long division

From the system of equations we observe that the arising remainders are the least positive residues of successive powers of 10 modulo 7. The seventh equation reveals that $10^6 \equiv 1 \pmod{7}$, a fact that we could have predicted by virtue of FLT. Observe also that at the seventh equation we meet the first repeated remainder, as 1 was also the remainder in the original equation. The relevance of this is that thereafter, the same sequence of equations must recur: the eighth equation is the second one again, and so on, explaining the cycling of the decimal.

There is nothing special about 7 here. For any natural number n , as there are only n residues modulo n , a remainder must repeat, and from this point onwards the sequence of equations recurs.

Exercise 2.1

Determine, by using the division algorithm, the decimal of (a) $\frac{1}{15}$ and (b) $\frac{1}{41}$.

Note that each q_i is one of the digits 0, 1, 2, ..., 9 since $0 \leq 10r_{i-1} < 10n$, and q_i is the quotient on dividing $10r_{i-1}$ by n .

$$\begin{aligned} 1 &= 0n + 1 \\ 10 &= q_1n + r_1 & 0 \leq r_1 < n \\ 10r_1 &= q_2n + r_2 & 0 \leq r_2 < n \\ 10r_2 &= q_3n + r_3 & 0 \leq r_3 < n \\ &\vdots \end{aligned}$$

The decimal of $\frac{1}{n}$ then begins $0.q_1q_2q_3\dots$. But it is the remainders r_i that tell us when recurrence will take place. As each of the remainders r_i is one of the n integers satisfying $0 \leq r_i < n$, there are at most n different equations here, and once a remainder appears for the second time subsequent equations repeat in a cycle.

Rearranging allows us to observe that $r_1 = 10 - q_1n \equiv 10 \pmod{n}$, and so $r_2 = 10r_1 - q_2n \equiv 10^2 \pmod{n}$. In fact we have

$$r_k \equiv 10^k \pmod{n}, \quad \text{for each } k.$$

One possibility that we have not considered is that remainder 0 arises. If this happens then the sequence of equations becomes, for some k ,

$$\begin{aligned} &\vdots \\ 10r_{k-2} &= q_{k-1}n + r_{k-1} \\ 10r_{k-1} &= q_kn + 0 \\ 0 &= 0n + 0 \\ &\vdots \end{aligned}$$

This is the situation corresponding to the terminating decimal. The last non-zero equation tells us that n divides $10r_{k-1}$, from which we deduce that n divides 10^k because $r_{k-1} \equiv 10^{k-1} \pmod{n}$. Now the factors of powers of 10 are those numbers whose only prime factors are 2 and/or 5, namely the numbers of the form 2^r5^s , where $r \geq 0$ and $s \geq 0$. Conversely, if $n = 2^r5^s$, then n divides 10^k where $k = \max\{r, s\}$ and the decimal of $\frac{1}{n}$ terminates after k decimal places. So the integers $1 < n < 100$ for which the decimal of $\frac{1}{n}$ terminates are $n = 2, 4, 5, 8, 10, 16, 20, 25, 32, 40, 50, 64$ and 80.

Before we move on to consider the case where the decimal does not terminate, let us record the following result.

Proposition 2.1 *Terminating decimals*

The decimal of $\frac{1}{n}$ terminates if, and only if, $n = 2^r 5^s$, for some integers $r \geq 0$ and $s \geq 0$.

2.2 The order of an integer

Let us turn to $\frac{1}{p}$ for p a prime other than 2 or 5. As $\text{hcf}(p, 10) = 1$, FLT tells us that $10^{p-1} \equiv 1 \pmod{p}$. The implication of this for the system of equations for $\frac{1}{p}$ is that the remainder in the p th equation is 1, and this will be a repeat of the remainder in the initial equation.

$$\begin{aligned} 1 &= 0 \times p + 1 \\ &\vdots \\ 10^{p-1} &\equiv 1 = 0 \times p + 1 \end{aligned}$$

So the decimal of $\frac{1}{p}$ has a cycle that begins immediately after the decimal point and that has length at most $p - 1$. We say that the length is *at most* $p - 1$ because, although we know that $10^{p-1} \equiv 1 \pmod{p}$, it might also be the case that $10^k \equiv 1 \pmod{p}$ for some smaller natural number k , and the remainder 1 would be repeated in an earlier equation. Indeed, we have already seen that this can happen. When $p = 11$ the decimal of $\frac{1}{11}$ is $0.\langle 09 \rangle$. As predicted, this has a cycle beginning at the first decimal place. But the length of this cycle is 2, rather than the suggested 10, because it is the case that $10^2 \equiv 1 \pmod{11}$. Similarly, in Exercise 2.1 you discovered that $\frac{1}{41}$ has a cycle of length 5. While FLT assured us that the cycle length could not exceed 40, since $10^{40} \equiv 1 \pmod{41}$, it is readily checked that $10^5 \equiv 1 \pmod{41}$.

All this suggests that we should look with interest at increasing positive powers of 10, searching for the first one that is congruent to 1 modulo p because this least exponent will give the length of the cycle in $\frac{1}{p}$. We refer to this least exponent as the *order* of 10 modulo p . The general definition is as follows.

Definition 2.2 *The order of an integer*

If p is prime and $\text{hcf}(a, p) = 1$, then the *order* of a modulo p is the least positive integer c such that $a^c \equiv 1 \pmod{p}$.

We should really say that *the decimal of $\frac{1}{41}$* has a cycle of length 5. However, when the meaning is clear we will often omit ‘the decimal of’ for brevity.

If $\text{hcf}(a, p) \neq 1$ then $a \equiv 0 \pmod{p}$ and so $a^c \equiv 0 \pmod{p}$ for all positive integers c . In this case there is no concept of order.

This definition assumes that for $\text{hcf}(a, p) = 1$ there is a unique least positive integer c such that $a^c \equiv 1 \pmod{p}$. This is guaranteed by FLT since $a^{p-1} \equiv 1 \pmod{p}$ gives $c \leq p - 1$.

With this terminology at our disposal, we can state formally what we have discovered about the cycle in $\frac{1}{p}$.

Proposition 2.3 *The cycle length of $\frac{1}{p}$*

The length of the cycle in the decimal of $\frac{1}{p}$ is equal to the order of 10 modulo p , where p is a prime other than 2 or 5.

Exercise 2.2

Determine the order of 10 modulo 17 and hence the length of the cycle of $\frac{1}{17}$.

We deal with primitive roots in general in Book C, Chapter 9. For our present purposes we are concerned only with cases where 10 is a primitive root of p .

Table 2.2 shows the order of 10 modulo each of the primes $p < 100$ (other than 2 and 5). Notice that for nine of these primes, the order of 10 modulo p is $p - 1$. When this occurs we say that 10 is a **primitive root** of p , and in this case the successive powers of 10 run through all the $p - 1$ non-zero residues of p in some order, as illustrated for the prime 17 in Exercise 2.2.

Table 2.2 The order of 10 modulo p for primes $p < 100$, other than 2 or 5

Prime p	Order of 10 modulo p	Prime p	Order of 10 modulo p
3	1	47	46
7	6	53	13
11	2	59	58
13	6	61	60
17	16	67	33
19	18	71	35
23	22	73	8
29	28	79	13
31	15	83	41
37	3	89	44
41	5	97	96
43	21		

This is the start of a much more extensive table that illustrates how, over the years, mathematicians have devoted large portions of their lives to calculations that can only be their own reward. In 1873 William Shanks (1812–1882) published an extension of this table covering all primes up to 30 000, and he subsequently progressed the table to all primes less than 120 000. To get some idea of how much calculation this involved – and remember that we are talking about the days long before electronic

calculating devices had landed on our desks – consider the prime 61. We know that $10^{60} \equiv 1 \pmod{61}$ and we need to confirm that there is no smaller natural number k for which $10^k \equiv 1 \pmod{61}$. In Exercise 2.2 we attacked a similar problem for the prime 17 by working out all the smaller powers of 10. However, there was no need to work them all out, as the following illustrates.

Exercise 2.3

Prove that if the order of 10 modulo 61 is c , then c is a factor of 60.

By virtue of Exercise 2.3, the order of 10 modulo 61 can be determined by finding the least positive residues, modulo 61, of the following powers of 10:

$$10, 10^2, 10^3, 10^4, 10^5, 10^6, 10^{10}, 10^{12}, 10^{15}, 10^{20} \text{ and } 10^{30}.$$

The required order is the exponent in the first of these that is congruent to 1 modulo 61. If, as turns out to be the case, none of them is congruent to 1 then the order of 10 is 60. This is a considerable improvement on having to determine all the first 60 powers of 10, but it still represents a considerable amount of computation; and all this is for just one relatively small prime. No doubt Shanks had a number of shortcuts available, but to achieve what he did by hand was no mean feat.

The result of Exercise 2.3 can be generalised, for there is nothing special about the prime 61. The proof of the following result, which we will use in Book C, Chapter 9, simply follows the argument given in the solution of Exercise 2.3.

Proposition 2.4

If a has order c modulo p , where $p \geq 3$ is prime, and $a^k \equiv 1 \pmod{p}$ then c is a factor of k .

In particular, c divides $p - 1$.

Proof By the Division Algorithm, we can write

$$k = qc + r, \quad \text{where } 0 \leq r < c.$$

Now

$$a^k = a^{qc+r} = (a^c)^q \times a^r \equiv 1^q \times a^r \equiv a^r \pmod{p}$$

and as $a^k \equiv 1 \pmod{p}$, $a^r \equiv 1 \pmod{p}$. Therefore $r = 0$, for otherwise the order of a would be less than c . Hence c divides k .

As FLT gives $a^{p-1} \equiv 1 \pmod{p}$, the order c divides $p - 1$. ■

2.3 Decimal representations of rational numbers

To determine the decimal of $\frac{2}{7}$ we proceed just as for $\frac{1}{7}$, but this time the first equation involves dividing 2 by 7.

$$\begin{array}{l} 2 = 0 \times 7 + 2 \\ 20 = 2 \times 7 + 6 \\ 60 = 8 \times 7 + 4 \\ 40 = 5 \times 7 + 5 \\ 50 = 7 \times 7 + 1 \\ 10 = 1 \times 7 + 3 \\ 30 = 4 \times 7 + 2 \end{array}$$


Notice that we get the same cycle of six equations as we had for $\frac{1}{7}$ but starting with a different equation. So the same six digits, in the same cyclic order but this time starting with the digit 2, form the cycle $\langle 285714 \rangle$ of $\frac{2}{7}$. In the same way you could check that $\frac{3}{7}$, $\frac{4}{7}$, $\frac{5}{7}$ and $\frac{6}{7}$ have decimals consisting of the same cycle of digits as that of $\frac{1}{7}$, but with appropriate starting points as shown below.

$$\begin{array}{l} \frac{1}{7} = 0.\langle 142857 \rangle \\ \frac{2}{7} = 0.\langle 285714 \rangle \\ \frac{3}{7} = 0.\langle 428571 \rangle \\ \frac{4}{7} = 0.\langle 571428 \rangle \\ \frac{5}{7} = 0.\langle 714285 \rangle \\ \frac{6}{7} = 0.\langle 857142 \rangle \end{array}$$

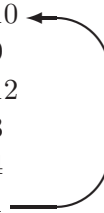
Although the proof of this result is not too demanding, we have opted not to include it here.

This situation is similar for any prime p having 10 as a primitive root. For such a prime the cycle of $\frac{1}{p}$ has length $p - 1$ and each $\frac{r}{p}$, for $r = 1, 2, \dots, p - 1$, has the same cycle of $p - 1$ digits but each with its own starting position.

Exercise 2.4

Given that $\frac{1}{17} = 0.\langle 0588235294117647 \rangle$, determine the decimals of $\frac{2}{17}$ and $\frac{9}{17}$.

We would be lacking in curiosity if we did not now ask whether or not any of this 'recycling' occurs when 10 is not a primitive root of prime p . Look at $p = 13$. In finding the decimal of $\frac{1}{13}$ we get the following set of equations.

$$\begin{array}{l} 1 = 0 \times 13 + 1 \\ 10 = 0 \times 13 + 10 \\ 100 = 7 \times 13 + 9 \\ 90 = 6 \times 13 + 12 \\ 120 = 9 \times 13 + 3 \\ 30 = 2 \times 13 + 4 \\ 40 = 3 \times 13 + 1 \end{array}$$


As the cycle has length 6, the order of 10 modulo 13 is 6 and so 10 is not a primitive root of 13. By taking each of its six starting points, these equations give the following six decimals:

$$\begin{aligned}\frac{1}{13} &= 0.\langle 076923 \rangle, \quad \frac{3}{13} = 0.\langle 230769 \rangle, \quad \frac{4}{13} = 0.\langle 307692 \rangle, \\ \frac{9}{13} &= 0.\langle 692307 \rangle, \quad \frac{10}{13} = 0.\langle 769230 \rangle, \quad \frac{12}{13} = 0.\langle 923076 \rangle.\end{aligned}$$

The numerator in each fraction is the remainder in the equation that precedes the start of the cycle.

In finding the decimal of $\frac{2}{13}$ we get the following set of equations.

$$\begin{aligned}2 &= 0 \times 13 + 2 \\ 20 &= 1 \times 13 + 7 \\ 70 &= 5 \times 13 + 5 \\ 50 &= 3 \times 13 + 11 \\ 110 &= 8 \times 13 + 6 \\ 60 &= 4 \times 13 + 8 \\ 80 &= 6 \times 13 + 2\end{aligned}$$


These equations give a second set of six decimals:

$$\begin{aligned}\frac{2}{13} &= 0.\langle 153846 \rangle, \quad \frac{5}{13} = 0.\langle 384615 \rangle, \quad \frac{6}{13} = 0.\langle 461538 \rangle, \\ \frac{7}{13} &= 0.\langle 538461 \rangle, \quad \frac{8}{13} = 0.\langle 615384 \rangle, \quad \frac{11}{13} = 0.\langle 846153 \rangle.\end{aligned}$$

There is nothing exceptional in this behaviour for the prime 13: it is typical of what happens for any prime p . Suppose that the order of 10 modulo p is c . It turns out that the decimals of $\frac{r}{p}$, for $1 \leq r < p$ form sets, each set consisting of c members with the same cycle of c digits varying only in their starting points. For example, consider $p = 41$. The order of 10 modulo 41 is 5 (see the solution of Exercise 2.1) and the 40 decimals $\frac{r}{41}$ have cycles of five digits. So these decimals will form eight sets, each set consisting of the same cycle but with the five different starting points. These are displayed in Table 2.3.

Table 2.3 The sets of cycles of $\frac{r}{41}$, for $1 \leq r < 41$

Set	Decimals				
1	$\frac{1}{41} = 0.\langle 02439 \rangle$	$\frac{10}{41} = 0.\langle 24390 \rangle$	$\frac{16}{41} = 0.\langle 39024 \rangle$	$\frac{18}{41} = 0.\langle 43902 \rangle$	$\frac{37}{41} = 0.\langle 90243 \rangle$
2	$\frac{2}{41} = 0.\langle 04878 \rangle$	$\frac{20}{41} = 0.\langle 48780 \rangle$	$\frac{32}{41} = 0.\langle 78048 \rangle$	$\frac{33}{41} = 0.\langle 80487 \rangle$	$\frac{36}{41} = 0.\langle 87804 \rangle$
3	$\frac{3}{41} = 0.\langle 07317 \rangle$	$\frac{7}{41} = 0.\langle 17073 \rangle$	$\frac{13}{41} = 0.\langle 31707 \rangle$	$\frac{29}{41} = 0.\langle 70731 \rangle$	$\frac{30}{41} = 0.\langle 73170 \rangle$
4	$\frac{4}{41} = 0.\langle 09756 \rangle$	$\frac{23}{41} = 0.\langle 56097 \rangle$	$\frac{25}{41} = 0.\langle 60975 \rangle$	$\frac{31}{41} = 0.\langle 75609 \rangle$	$\frac{40}{41} = 0.\langle 97560 \rangle$
5	$\frac{5}{41} = 0.\langle 12195 \rangle$	$\frac{8}{41} = 0.\langle 19512 \rangle$	$\frac{9}{41} = 0.\langle 21951 \rangle$	$\frac{21}{41} = 0.\langle 51219 \rangle$	$\frac{39}{41} = 0.\langle 95121 \rangle$
6	$\frac{6}{41} = 0.\langle 14634 \rangle$	$\frac{14}{41} = 0.\langle 34146 \rangle$	$\frac{17}{41} = 0.\langle 41463 \rangle$	$\frac{19}{41} = 0.\langle 46341 \rangle$	$\frac{26}{41} = 0.\langle 63414 \rangle$
7	$\frac{11}{41} = 0.\langle 26829 \rangle$	$\frac{12}{41} = 0.\langle 29268 \rangle$	$\frac{28}{41} = 0.\langle 68292 \rangle$	$\frac{34}{41} = 0.\langle 82926 \rangle$	$\frac{38}{41} = 0.\langle 92682 \rangle$
8	$\frac{15}{41} = 0.\langle 36585 \rangle$	$\frac{22}{41} = 0.\langle 53658 \rangle$	$\frac{24}{41} = 0.\langle 58536 \rangle$	$\frac{27}{41} = 0.\langle 65853 \rangle$	$\frac{35}{41} = 0.\langle 85365 \rangle$

We leave decimals at this point, aware that there are further areas for investigation. In particular, we have not pursued reciprocals of composite numbers, other than to recognise which ones terminate. As a parting

A **proper fraction** is one of the form $\frac{m}{n}$, where $\text{hcf}(m, n) = 1$; that is, a fraction in which all common factors of the numerator and denominator have been cancelled.

observation, we mention that the decimal of $\frac{1}{49}$ is a cycle of length 42:

$$\frac{1}{49} = 0.\langle 020408163265306122448979591836734693877551 \rangle,$$

and that the 42 decimals obtained from this cycle by letting each digit of the cycle lead are the proper fractions $\frac{k}{49}$, where $1 \leq k < 49$; that is, those with $\text{hcf}(k, 49) = 1$. For example,

$$\frac{11}{49} = 0.\langle 224489795918367346938775510204081632653061 \rangle.$$

However, of all composite integers less than 100, 49 is the only one that exhibits this elegant behaviour of its proper fractions. The relevance of the cycle length of $\frac{1}{49}$ will become apparent once you have met Euler's generalisation of FLT, in Book C, Chapter 9.

Exercise 2.5

- (a) Leibniz claimed, in 1677, that for any natural number n with $\text{hcf}(n, 10) = 1$, the length of the cycle of $\frac{1}{n}$ is a factor of $n - 1$. Determine the decimal fraction for $\frac{1}{21}$ and prove him wrong.
- (b) From Proposition 2.3 it can be deduced that for each natural number n , there are at most a finite number of primes p for which the length of the cycle of $\frac{1}{p}$ is n . Explain how.
- (c) By first determining the prime decomposition of $10^4 - 1$, find all the primes p for which $\frac{1}{p}$ has a cycle of length 4. From the decomposition of $10^6 - 1$, find all primes p for which $\frac{1}{p}$ consists of a cycle of length 6.
- (d) Consider an ordinary pack of 52 playing cards. In the **perfect faro shuffle** the pack is cut into two equal halves, which are then placed (flicked) alternately, as illustrated in Figure 2.2.

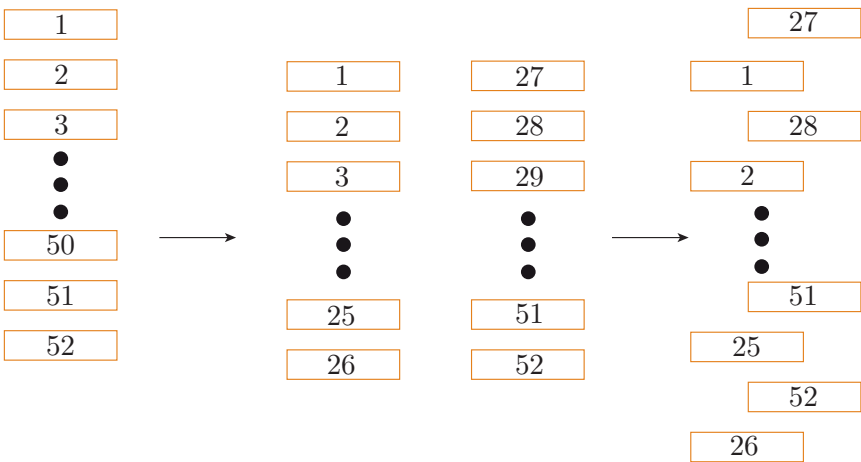


Figure 2.2 The perfect faro shuffle

The cards that initially occupy positions 1, 2, ..., 26 are moved to positions 2, 4, ..., 52 whilst the cards initially in positions 27, 28, ..., 52 are moved to positions 1, 3, ..., 51. Thus the card starting at position x moves to position y , where $1 \leq y \leq 52$ and

$y \equiv 2x \pmod{53}$. After n such shuffles this card will occupy position $2^n x \pmod{53}$.

- (i) After how many perfect faro shuffles will the pack return to its initial order for the first time?
- (ii) If two jokers are included in the pack, making 54 cards in all, after how many perfect faro shuffles would this pack be restored to the original order for the first time?

3 Wilson's Theorem

Let us turn now to a result that is not of very much practical use but one that, nevertheless, has a prominent place in the development of number theory. The English mathematician Edward Waring (c.1736–1798) reported, in his book *Meditationes Algebraicae* (1770), a result claimed by one of his former students, John Wilson (1741–1793). Wilson had asserted that for each prime p , the number

$$\frac{(p-1)! + 1}{p}$$

is an integer. Wilson appears to have guessed the result on empirical evidence, for neither he nor Waring could supply a proof. But shortly afterwards, the French mathematician Lagrange (1736–1813) gave a proof of the result. Throughout mathematical literature the result has become known as Wilson's Theorem, although a manuscript written in 1682 indicates that Leibniz was aware of the result, and how to prove it, long before Wilson came on the scene.

The language of congruence gives us a neater way of expressing the result.

Theorem 3.1 Wilson's Theorem

If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

First we look at the particular case of the prime 17 to illustrate the idea behind the proof that we are going to give. For $p = 17$ the theorem claims that $16! \equiv -1 \pmod{17}$.

To evaluate $16!$ we could multiply together the sixteen numbers from 1 to 16 inclusive, reducing the answer modulo 17. But notice how the numbers from 2 to 15 inclusive pair up so that their product is congruent to 1 modulo 17.

$$\begin{array}{ll} 2 \times 9 \equiv 1 \pmod{17} & 3 \times 6 \equiv 1 \pmod{17} \\ 4 \times 13 \equiv 1 \pmod{17} & 5 \times 7 \equiv 1 \pmod{17} \\ 8 \times 15 \equiv 1 \pmod{17} & 10 \times 12 \equiv 1 \pmod{17} \\ 11 \times 14 \equiv 1 \pmod{17} & \end{array}$$

This observation gives us that

$$\begin{aligned} 15! &= 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \times 13 \times 14 \times 15 \\ &\equiv 1^7 \equiv 1 \pmod{17}, \end{aligned}$$

and so

$$16! = 15! \times 16 \equiv 1 \times 16 = 16 \equiv -1 \pmod{17}.$$

The substance of our general proof lies in showing that this convenient pairing of factors in $(p-2)!$ always occurs. This particular proof was first given by Gauss.

Proof of Wilson's Theorem (Theorem 3.1) The observations $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$ confirm the result for $p = 2$ and $p = 3$, so we can confine attention to $p \geq 5$.

Consider the set of $p-3$ integers $S = \{2, 3, 4, \dots, p-2\}$. If $a \in S$ then, as $\text{hcf}(a, p) = 1$, the linear congruence $ax \equiv 1 \pmod{p}$ has, by Theorem 3.4 of Chapter 3, a *unique* least positive solution modulo p . Let the solution be a' , so that $aa' \equiv 1 \pmod{p}$. Now $a' \neq 1$ because $a' = 1$ would give $a \equiv 1 \pmod{p}$, contradicting $a \in S$. Similarly $a' \neq p-1$ because $a' = p-1$ would imply $a \equiv -1 \pmod{p}$, again contradicting $a \in S$. Hence $a' \in S$.

Finally $a \neq a'$, for otherwise $aa' = a^2 \equiv 1 \pmod{p}$, which would give that p divides $a^2 - 1$. But then p divides $(a-1)(a+1)$, whereupon Euclid's Lemma gives p divides $a-1$ or p divides $a+1$, which amount to $a = 1$ or $a = p-1$ respectively, each of which contradicts $a \in S$.

We conclude that for each element $a \in S$ there is a unique element $a' \in S$, $a \neq a'$, for which $aa' \equiv 1 \pmod{p}$. Thus the elements of S form $\frac{p-3}{2}$ distinct pairs a and a' with $aa' \equiv 1 \pmod{p}$. Multiplying these congruences together, each element of S is involved exactly once, and so

$$2 \times 3 \times 4 \times \cdots \times (p-2) \equiv 1 \pmod{p}.$$

Multiplying both sides of this congruence by $(p-1)$ gives

$$2 \times 3 \times 4 \times \cdots \times (p-2) \times (p-1) \equiv p-1 \pmod{p},$$

that is,

$$(p-1)! \equiv -1 \pmod{p},$$

completing the proof. ■

The converse of Wilson's Theorem is also true, and its proof is relatively simple.

Proposition 3.2 *Converse of Wilson's Theorem*

If $n > 1$ is an integer and $(n-1)! \equiv -1 \pmod{n}$ then n is prime.

Note that $p-3$ is even as p is odd.

Proof Suppose that n divides $(n-1)! + 1$. Let r be a positive factor of n , where $r < n$. Then as

$$(n-1)! = 1 \times 2 \times 3 \times \cdots \times r \times \cdots \times (n-1),$$

r divides $(n-1)!$. But r divides $(n-1)! + 1$, and so r divides 1, from which we conclude that $r = 1$. That is, n has no positive factors other than itself and 1, and therefore is prime. ■

Exercise 3.1

Find the smallest prime factor of:

- (a) $18! + 1$
- (b) $29! - 1$.

Wilson's Theorem and its converse together give a characterisation of prime numbers: $n > 1$ is prime if, and only if, n divides $(n-1)! + 1$. Unfortunately it is not of much practical use because of the amount of computation that would be involved in using it. For instance, to prove that 43 is prime by this method involves checking whether or not $42! + 1$ is divisible by 43. Even working modulo 43, the evaluation of $42!$ is quite demanding, and that is for a relatively small prime. However, Wilson's Theorem can be put to work in other ways. In the next worked exercise it is used to discover a solution of a *quadratic congruence*. The theory of quadratic congruences has great importance in number theory and we devote a substantial part of Book C, Chapter 10 to its study.

Worked Exercise 3.3

Show that the congruence $x^2 + 1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if, and only if, $p \equiv 1 \pmod{4}$.

Solution

We first use Wilson's Theorem to show that the congruence has a solution when $p = 4k + 1$. In this case $(p-1)! = (4k)! \equiv -1 \pmod{4k+1}$. That is,

$$\begin{aligned} (p-1)! &= 1 \times 2 \times 3 \times \cdots \times (2k) \times (2k+1) \times \cdots \times (4k-1) \times (4k) \\ &\equiv -1 \pmod{4k+1}. \end{aligned}$$

Now, working modulo $4k+1$ we have

$$\begin{aligned} 4k &\equiv -1 \\ 4k-1 &\equiv -2 \\ &\vdots \\ 2k+1 &\equiv -2k, \end{aligned}$$

and substituting these values into the expression for $(p-1)!$ we obtain

$$\begin{aligned}
 -1 &\equiv (p-1)! \pmod{4k+1} \\
 &\equiv 1 \times 2 \times \cdots \times (2k) \times (-2k) \times \cdots \times (-2) \times (-1) \pmod{4k+1} \\
 &\equiv 1 \times 2 \times \cdots \times (2k) \times (-1)^{2k} \times (2k) \times \cdots \times 2 \times 1 \pmod{4k+1} \\
 &\equiv 1^2 \times 2^2 \times \cdots \times (2k)^2 \pmod{4k+1} \\
 &\equiv ((2k)!)^2 \pmod{4k+1}.
 \end{aligned}$$

Hence $x = (2k)!$ satisfies $x^2 + 1 \equiv 0 \pmod{4k+1}$ and so the congruence has a solution.

We now show that if $p \not\equiv 1 \pmod{4}$ then there is no solution. In this case the odd prime is of the form $4k+3$. Heading for a contradiction, suppose that the congruence $x^2 + 1 \equiv 0 \pmod{4k+3}$ has a solution; that is, there is an integer a such that $a^2 \equiv -1 \pmod{4k+3}$. Then, applying FLT for prime $4k+3$,

$$a^{4k+2} \equiv 1 \pmod{4k+3}.$$

But

$$a^{4k+2} = (a^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{4k+3},$$

giving the contradiction $1 \equiv -1 \pmod{4k+3}$.

Exercise 3.2

- (a) Find two solutions of the quadratic congruence $x^2 + 1 \equiv 0 \pmod{29}$.
- (b) Prove that, for each odd prime p ,

$$\begin{aligned}
 1^2 \times 3^2 \times \cdots \times (p-2)^2 &\equiv 2^2 \times 4^2 \times \cdots \times (p-1)^2 \\
 &\equiv (-1)^{(p+1)/2} \pmod{p}.
 \end{aligned}$$

Hint: use Wilson's Theorem together with the fact that $2k \equiv -(p-2k) \pmod{p}$.

As a final deduction from Wilson's Theorem, we observe that it tells us that there are infinitely many integers n for which $n! + 1$ is composite: simply choose $n = p-1$ for any prime $p > 3$.

To see this, note that p is known to be a factor of $(p-1)! + 1$, implying that the latter is composite except when $(p-1)! + 1 = p$. This condition occurs only for $p = 2$ and $p = 3$.

For other values of n the number $n! + 1$ may be either prime or composite, and it remains an unanswered question as to whether or not there are infinitely many primes of the form $n! + 1$. For values of n up to 100, those for which $n! + 1$ is prime are $n = 1, 2, 3, 11, 27, 37, 41, 73$ and 77 .

Exercise 3.3

- (a) If, for some a , the numbers $a, a^2, a^3, \dots, a^{p-2}$ are congruent modulo p to the numbers $2, 3, 4, \dots, p-1$, in some order, then it follows that the order of a modulo p is $p-1$ (that is, a is a primitive root of p). In particular, observe that

$$a^k a^{p-k-1} = a^{p-1} \equiv 1 \pmod{p}.$$

Show that the order of 2 modulo 29 is 28 and use the given observation to find the distribution of $\{2, 3, \dots, 27\}$ into 13 pairs in such a way that the product of each pair is congruent to 1 modulo 29. Hence illustrate the proof of Wilson's Theorem for the prime 29.

- (b) If p is a prime and a is any integer, prove that p divides both

$$a^p + a \times (p-1)! \quad \text{and} \quad a + a^p \times (p-1)!$$

- (c) For p prime, prove that

$$(p-1)! \equiv p-1 \pmod{1+2+3+\dots+(p-1)}.$$

4 Polynomial congruences

In Chapter 3 we saw how to solve linear congruences. Here, with the help of Fermat's Little Theorem and Wilson's Theorem, we will explore solutions for polynomial congruences of higher degree.

4.1 Lagrange's Theorem

In preparation for the investigation of linear congruences in Chapter 3, we briefly introduced the notion of polynomial congruences and their solutions. For convenience we reiterate the definitions here.

Definition 4.1 *Polynomial congruences and their solutions*

A polynomial congruence is an expression

$$P(x) = c_r x^r + c_{r-1} x^{r-1} + \dots + c_1 x + c_0 \equiv 0 \pmod{n},$$

where $P(x)$ is a polynomial of degree $r \geq 0$ with integer coefficients.

An integer a is a solution of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ if, and only if, $P(a) \equiv 0 \pmod{n}$.

The number of solutions of a polynomial congruence is the number of incongruent solutions modulo n .

In the congruence context we are concerned exclusively with integers, and consequently we are forced to restrict attention to polynomials with integer coefficients. Hence, in this section, when we mention a polynomial it will be assumed that it has integer coefficients.

It follows from these definitions that the polynomial congruence $P(x) \equiv 0 \pmod{n}$ has at most n solutions, and these could be discovered by finding which integers in a complete set of residues, such as $\{0, 1, 2, \dots, n-1\}$, are solutions.

Exercise 4.1

Solve the following polynomial congruences.

- (a) $x^3 - x \equiv 0 \pmod{6}$
- (b) $x^3 - x \equiv 0 \pmod{8}$
- (c) $x^2 + x + 1 \equiv 0 \pmod{7}$
- (d) $2x^2 + 9x + 15 \equiv 0 \pmod{7}$

Now consider the polynomial congruence

$$x^{20} + 3x^{14} + 8x^{10} + 3x^2 + 6 \equiv 0 \pmod{7}.$$

This still may not appear too daunting. After all, we could solve the congruence by exhaustion, evaluating the left-hand side for $x = 0, 1, 2, 3, 4, 5$ and 6 . But even that involves a good deal of computation, and if we change the modulus to something significantly larger this approach would be impractical. What we need is a more sophisticated, systematic approach, and here FLT comes to our aid.

FLT informs us that, for all integers x , $x^7 \equiv x \pmod{7}$, and so

$$x^{20} = (x^7)^2 x^6 \equiv x^2 x^6 = x^7 x \equiv x^2 \pmod{7}.$$

Similarly, $x^{14} \equiv x^2 \pmod{7}$ and $x^{10} \equiv x^4 \pmod{7}$. Therefore solving the original congruence is equivalent to solving

$$x^2 + 3x^2 + 8x^4 + 3x^2 + 6 \equiv 8x^4 + 7x^2 + 6 \equiv 0 \pmod{7}.$$

Simplifying further by reducing the coefficients, $8 \equiv 1 \pmod{7}$, etc., we arrive at the equivalent congruence

$$x^4 - 1 \equiv 0 \pmod{7}.$$

Checking the fourth powers of $0, \pm 1, \pm 2$ and ± 3 , we find that the congruence has just the two solutions $x \equiv \pm 1 \pmod{7}$.

This example illustrates a useful role for FLT in solving polynomial congruences, offering the possibility of replacing the polynomial in question with one of smaller degree. We are not going to develop any general theory for solving such congruences here but, rather, just touch the beginnings of the subject through examples. What we will find is that when working to a modulus that is not prime, unexpected and unwanted things can happen; but when the modulus is prime the situation is more clear-cut. Our

principal goal is a theorem of Lagrange that gives an insight into the number of solutions to a polynomial congruence with prime modulus.

One well-known principle from the theory of equations, the so-called Fundamental Theorem of Algebra, asserts that a polynomial equation of degree n with real coefficients has at the most n roots (solutions). We already have evidence that the same principle cannot hold for polynomial congruences; for example, we witnessed in Exercise 4.1 a polynomial of degree 3 for which the associated congruence modulo 6 has more than three solutions. Indeed, we have seen that linear congruences (degree 1) do not necessarily have unique solutions; the congruence $2x \equiv 2 \pmod{4}$ has the two solutions $x \equiv 1, 3 \pmod{4}$. However, looking back through the examples at hand, wherever the modulus is a prime this ‘misbehaviour’ does not occur. Lagrange, in 1768, proved that the number of solutions of a polynomial congruence in which the modulus is prime is less than or equal to its degree.

But first we must clarify what we mean by the degree of a polynomial congruence. Consider the following congruence:

$$7x^3 + 4x^2 - 3 \equiv 0 \pmod{7}.$$

The polynomial involved has degree 3. However, when we turn to congruence modulo 7, the leading term, $7x^3$, vanishes since $7 \equiv 0 \pmod{7}$. Hence, modulo 7, this polynomial has degree 2 because the leading term with non-zero coefficient modulo 7 is $4x^2$.

By the *leading term* in a polynomial $P(x)$ we mean the (non-zero) term involving the highest power of x . By ‘non-zero modulo n ’ we mean ‘not congruent to zero modulo n ’.

Definition 4.2 Degree of a polynomial congruence

If $P(x) = c_r x^r + c_{r-1} x^{r-1} + \cdots + c_1 x + c_0$ then the polynomial $P(x)$ has degree k modulo n if, after removing each term in which the coefficient $c_i \equiv 0 \pmod{n}$, the leading term remaining is $c_k x^k$.

If every coefficient $c_i \equiv 0 \pmod{n}$ then the polynomial is not assigned a degree modulo n .

The degree of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ is the degree of $P(x)$ modulo n .

Exercise 4.2

What are the degrees of the following polynomial congruences?

- (a) $3x^6 + 7x^2 - 2 \equiv 0 \pmod{5}$
- (b) $10x^3 + 3x + 1 \equiv 0 \pmod{5}$
- (c) $15x^2 - 10x + 2 \equiv 0 \pmod{5}$

We are now ready to state our main result of this section. Its proof will come in the next subsection.

Theorem 4.3 Lagrange's Theorem

Let p be a prime. A polynomial congruence $P(x) \equiv 0 \pmod{p}$ of degree $k \geq 1$ can have at most k solutions.

4.2 Factorising polynomial congruences

The proof that we give for Lagrange's Theorem follows closely one of the methods of proving the Fundamental Theorem of Algebra in which the polynomial $P(x)$ is effectively factorised. To this end we will first prove a subsidiary result that introduces the idea of factors in polynomial congruences.

Lemma 4.4

Let b be a solution of the polynomial congruence $P(x) \equiv 0 \pmod{p}$ of degree $k \geq 1$. Then $P(x) \equiv (x - b)P_1(x) \pmod{p}$, where $P_1(x)$ is a polynomial of degree $k - 1$ modulo p .

Proof Suppose that $P(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0$, where $c_k \not\equiv 0 \pmod{p}$. Since $P(b) \equiv 0 \pmod{p}$, we have $P(x) \equiv P(x) - P(b) \pmod{p}$. Now

$$P(x) - P(b) = c_k(x^k - b^k) + c_{k-1}(x^{k-1} - b^{k-1}) + \cdots + c_1(x - b).$$

Each term in the sum on the right-hand side has a factor $(x - b)$ since

$$x^r - b^r = (x - b)(x^{r-1} + bx^{r-2} + b^2x^{r-3} + \cdots + b^{r-2}x + b^{r-1}).$$

Hence

$$P(x) \equiv P(x) - P(b) \equiv (x - b)P_1(x) \pmod{p},$$

where the polynomial $P_1(x)$ has integer coefficients and leading term $c_k x^{k-1}$. As $c_k \not\equiv 0 \pmod{p}$, $P_1(x)$ has degree $k - 1$ modulo p . ■

In the statement of Lemma 4.4 we called the modulus p , but we did not stipulate that p was prime. Indeed, the above proof holds true for p composite. However, when we progress from a single factor to our next result, which pulls out a factor for each solution of the congruence, we do need the modulus to be prime.

Proposition 4.5 *Factorising a polynomial modulo p*

Let p be prime and let $b_1, b_2, \dots, b_r$ be incongruent solutions of the polynomial congruence $P(x) \equiv 0 \pmod{p}$ of degree $k \geq r$. Then

$$P(x) \equiv (x - b_1)(x - b_2) \cdots (x - b_r)P_r(x) \pmod{p},$$

where the polynomial $P_r(x)$ has degree $k - r$ modulo p .

Proof Lemma 4.4 tells us that $P(x) \equiv (x - b_1)P_1(x) \pmod{p}$, where $P_1(x)$ has degree $k - 1$ modulo p . Now $P(b_2) \equiv 0 \pmod{p}$, and so

$$(b_2 - b_1)P_1(b_2) \equiv 0 \pmod{p}.$$

But p does not divide $b_2 - b_1$, since b_1 and b_2 are incongruent solutions modulo p . Hence $P_1(b_2) \equiv 0 \pmod{p}$ by Euclid's Lemma. This allows us to invoke Lemma 4.4 again:

$$P_1(x) \equiv (x - b_2)P_2(x) \pmod{p},$$

where $P_2(x)$ has degree $k - 2$ modulo p .

Substituting for $P_1(x)$ gives

$$P(x) \equiv (x - b_1)(x - b_2)P_2(x) \pmod{p}.$$

Continuing, from $P(b_3) \equiv 0 \pmod{p}$ we deduce that $P_2(b_3) \equiv 0 \pmod{p}$ and hence that

$$P_2(x) \equiv (x - b_3)P_3(x) \pmod{p},$$

where $P_3(x)$ has degree $k - 3$ modulo p .

The desired result is reached when all r incongruent solutions have been processed in this way. ■

This is where we require the modulus p to be prime.

Let us look at a worked exercise to illustrate the proof of Proposition 4.5.

Worked Exercise 4.6

Let $P(x) = x^4 - x^3 + 5x^2 - 3x - 2$. Confirm that $x \equiv 1, 3 \pmod{11}$ are two solutions of $P(x) \equiv 0 \pmod{11}$ and find $P_2(x)$ such that $P(x) \equiv (x - 1)(x - 3)P_2(x) \pmod{11}$.

Solution

$$P(1) = 1 - 1 + 5 - 3 - 2 \equiv 0 \pmod{11}$$

and

$$P(3) = 81 - 27 + 45 - 9 - 2 = 88 \equiv 0 \pmod{11},$$

so both are solutions as claimed.

Writing

$$x^4 - x^3 + 5x^2 - 3x - 2 \equiv (x - 1)(Ax^3 + Bx^2 + Cx + D) \pmod{11},$$

we can solve for A , B , C and D by looking at the various powers of x and equating coefficients modulo 11.

$$x^4 : \quad 1 \equiv A$$

$$x^3 : \quad -1 \equiv -A + B, \text{ giving } B \equiv 0$$

$$x^2 : \quad 5 \equiv -B + C, \text{ giving } C \equiv 5$$

$$x : \quad -3 \equiv -C + D, \text{ giving } D \equiv 2$$

$$\text{constant : } -2 \equiv -D, \text{ which provides a check.}$$

$$\text{So } x^4 - x^3 + 5x^2 - 3x - 2 \equiv (x - 1)(x^3 + 5x + 2) \pmod{11}.$$

Now $x \equiv 3 \pmod{11}$ is a solution of $x^3 + 5x + 2 \equiv 0 \pmod{11}$ and so

$$x^3 + 5x + 2 \equiv (x - 3)(Ex^2 + Fx + G) \pmod{11}.$$

We can solve this in the same way as above to get $E \equiv 1$, $F \equiv 3$, $G \equiv 3 \pmod{11}$.

Hence

$$x^4 - x^3 + 5x^2 - 3x - 2 \equiv (x - 1)(x - 3)(x^2 + 3x + 3) \pmod{11}.$$

Aside: In fact, the quadratic $x^2 + 3x + 3$ cannot be factorised modulo 11. In just the same way as a quadratic equation might have 0, 1 or 2 real solutions, it turns out that a quadratic congruence with prime modulus can have 0, 1 or 2 solutions. The quadratic congruence

$$x^2 + 3x + 3 \equiv 0 \pmod{11}$$

has no solutions.

Exercise 4.3

For each of the following polynomials $P(x)$, find all the solutions of $P(x) \equiv 0 \pmod{7}$ by exhaustion, and hence factorise the polynomial modulo 7.

(a) $x^2 + 4x - 4$

(b) $x^3 + 2x^2 + x + 3$

If we apply Proposition 4.5 to one particular polynomial, we get a result that is well worth recording.

Corollary 4.7 to Proposition 4.5

For any prime p ,

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3) \cdots (x-(p-1)) \pmod{p}.$$

Proof Consider the congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

FLT uncovers $p-1$ incongruent solutions since this congruence is satisfied by $x = 1, 2, 3, \dots, p-1$. Hence, applying Proposition 4.5,

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3) \cdots (x-(p-1))Q(x) \pmod{p},$$

where $Q(x)$ has degree $p-1-(p-1) = 0$ modulo p . So $Q(x)$ is a constant polynomial. Inspection of the coefficient of x^{p-1} confirms that $Q(x) \equiv 1 \pmod{p}$, as required. ■

It would be remiss of us not to record what happens when x is taken to be 0 in the corollary.

For any prime p ,

$$\begin{aligned} 0 - 1 &\equiv (-1)(-2) \cdots (-(p-1)) \pmod{p} \\ &\equiv (-1)^{p-1}(p-1)! \pmod{p} \\ &\equiv (p-1)! \pmod{p}, \quad \text{since } p-1 \text{ is even or} \\ &\quad p = 2 \text{ in which case } -1 \equiv 1 \pmod{p}. \end{aligned}$$

That is,

$$(p-1)! \equiv -1 \pmod{p},$$

which is Wilson's Theorem.

The result of Proposition 4.5 is the backbone of our proof of Lagrange's Theorem. We simply have to draw the right conclusions from our ability to pull out a linear factor corresponding to each solution of the congruence.

Proof of Lagrange's Theorem Suppose to the contrary that a polynomial congruence $P(x) \equiv 0 \pmod{p}$ has degree k but has incongruent solutions $b_1, b_2, \dots, b_k$ and b_{k+1} . Applying Proposition 4.5 for the first k solutions, we have that

$$P(x) \equiv (x-b_1)(x-b_2) \cdots (x-b_k)P_k(x) \pmod{p},$$

where $P_k(x)$ has degree $k-k$ modulo p . Having degree 0, $P_k(x)$ is a constant polynomial, say, $P_k(x) = a$. Notice that the leading term in $P(x)$ modulo p is ax^k and so, as $P(x)$ has degree k modulo p , $a \not\equiv 0 \pmod{p}$.

The constant a is just the coefficient c_k of Definition 4.2.

Now consider the further solution b_{k+1} :

$$P(b_{k+1}) \equiv (b_{k+1}-b_1)(b_{k+1}-b_2) \cdots (b_{k+1}-b_k)a \equiv 0 \pmod{p}.$$

This means that p divides $(b_{k+1}-b_1)(b_{k+1}-b_2) \cdots (b_{k+1}-b_k)a$ and so, p being prime, Euclid's Lemma implies that p divides one of the terms $b_{k+1}-b_i$ or p divides a . But neither of these is possible: p cannot divide

$b_{k+1} - b_i$ as the solutions are incongruent modulo p , and we have seen that $a \not\equiv 0 \pmod{p}$.

What has been contradicted? The only assumption made is that the polynomial congruence of degree k has $k + 1$ solutions. This therefore cannot happen and our proof is complete. ■

It is illuminating to see what happens when the modulus is not prime. Consider again the polynomial congruence

$$x^3 - x \equiv 0 \pmod{6},$$

which we found, in Exercise 4.1, to have six solutions. One factorisation of the polynomial $x^3 - x$ is readily spotted:

$$x^3 - x = x(x^2 - 1) = x(x - 1)(x + 1) \equiv 0 \pmod{6}.$$

Each of the three discovered factors suggests a solution of the congruence: $x \equiv 0, 1$ and $-1 \pmod{6}$ respectively. But $x \equiv 2, 3$ and $4 \pmod{6}$ are also solutions, and the factorisation has not contradicted this. For example, putting $x = 4$ into the factorised polynomial gives

$$4(4 - 1)(4 + 1) = 60 \equiv 0 \pmod{6},$$

and so the solution $x \equiv 4 \pmod{6}$ has not gone away!

The problem is that, since 6 is composite, we cannot deduce from $x(x - 1)(x + 1) \equiv 0 \pmod{6}$ that $x \equiv 0 \pmod{6}$, or $(x - 1) \equiv 0 \pmod{6}$ or $(x + 1) \equiv 0 \pmod{6}$. The corresponding deduction in Lagrange's Theorem could be made because the modulus was prime, and this was the key to relating factors of the polynomial to solutions of the congruence.

Notice that since $x \equiv 4 \pmod{6}$ is a solution of this congruence, Lemma 4.4 claims that $x - 4$ can be pulled out as a factor on the left-hand side of $x^3 - x \equiv 0 \pmod{6}$. Indeed it can, showing that the one factorisation that we wrote down above is not the only one!

$$\begin{aligned} x^3 - x &\equiv (x - 4)(x^2 + 4x + 3) \pmod{6} \\ &\equiv (x - 4)(x + 1)(x + 3) \pmod{6}. \end{aligned}$$

There are other ways of writing $x^3 - x$ as a product of three linear factors to which it is congruent modulo 6.

To complete the theoretical results of the section, we give an interesting consequence of Lagrange's Theorem.

Proposition 4.8

If p is prime and d is a factor of $p - 1$ then the congruence

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Proof Let $p - 1 = dr$ for some integer r . If $r = 1$ then $d = p - 1$ and the result follows from Corollary 4.7. We may assume therefore that $r \geq 2$. Then

$$\begin{aligned} x^{p-1} - 1 &= (x^d - 1)(x^{d(r-1)} + x^{d(r-2)} + \cdots + x^d + 1) \\ &= (x^d - 1)Q(x), \end{aligned}$$

where $Q(x)$ has degree $d(r - 1)$ modulo p .

Now we know from Corollary 4.7 that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p - 1$ solutions. If a is such a solution then

$$a^{p-1} - 1 = (a^d - 1)Q(a) \equiv 0 \pmod{p},$$

from which Euclid's Lemma informs us that either $(a^d - 1) \equiv 0 \pmod{p}$ or $Q(a) \equiv 0 \pmod{p}$. In other words, any solution of $x^{p-1} - 1 \equiv 0 \pmod{p}$ is necessarily a solution of either $x^d - 1 \equiv 0 \pmod{p}$ or $Q(x) \equiv 0 \pmod{p}$. Hence these latter two congruences have, between them, at least $p - 1$ solutions.

Now apply Lagrange's Theorem. The congruence $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions and $Q(x) \equiv 0 \pmod{p}$ has at most $d(r - 1)$ solutions. So between them they have at most

$$d + d(r - 1) = dr = p - 1$$

solutions. It follows that they have, between them, exactly $p - 1$ solutions and, in particular, $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions. ■

4.3 Congruences with composite moduli

This section has been mainly concerned with theoretical results concerning polynomial congruences rather than with developing techniques for actually solving the congruences. For our purposes in this module, we will not have a great need to solve anything other than relatively simple congruences. We have seen that for not too large a prime modulus we can, failing anything better, attack congruences by an exhaustive method involving evaluation of the polynomial over a complete set of residues. To round off the section, we look at a couple of more complicated examples with composite moduli that illustrate general lines of attack.

Consider the polynomial congruence $P(x) \equiv 0 \pmod{m}$, where $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. If a is a solution of this congruence then $P(a) \equiv 0 \pmod{m}$ and so $P(a) \equiv 0 \pmod{p_i^{k_i}}$ for each of the prime factors. It follows that any solution of $P(x) \equiv 0 \pmod{m}$ must be a simultaneous solution of the r polynomial congruences $P(x) \equiv 0 \pmod{p_i^{k_i}}$. Conversely, if a is a simultaneous solution of the r polynomial congruences then by repeated application of the corollary to Theorem 1.6 of Chapter 3, a is a solution of $P(x) \equiv 0 \pmod{m}$. So if we solve, individually, each of the congruences involving a single prime, we can then use the Chinese Remainder Theorem to build a solution of the original congruence. Here is a simple example.

Worked Exercise 4.9

Solve $2x^2 + 5x - 3 \equiv 0 \pmod{72}$.

Solution

As $72 = 2^3 \times 3^2$, we first solve $2x^2 + 5x - 3 \equiv 0 \pmod{8}$ and $2x^2 + 5x - 3 \equiv 0 \pmod{9}$. Trying all eight possibilities for the first congruence and all nine for the second, we discover that

$$2x^2 + 5x - 3 \equiv 0 \pmod{8} \text{ has unique solution } x \equiv 5 \pmod{8}$$

and

$$2x^2 + 5x - 3 \equiv 0 \pmod{9} \text{ has solutions } x \equiv 5, 6 \pmod{9}.$$

The congruence $2x^2 + 5x - 3 \equiv 0 \pmod{72}$ therefore has two solutions:

- (a) the simultaneous solution of $x \equiv 5 \pmod{8}$ and $x \equiv 5 \pmod{9}$, namely

$$x \equiv 5 \pmod{72}, \text{ and}$$

- (b) the simultaneous solution of $x \equiv 5 \pmod{8}$ and $x \equiv 6 \pmod{9}$, namely

$$x \equiv 69 \pmod{72}.$$

Exercise 4.4

Solve $x^2 - x + 4 \equiv 0 \pmod{80}$.

We have now reduced the problem of solving polynomial congruences to the task of solving $P(x) \equiv 0 \pmod{p^k}$ for prime p . In fact, all solutions of this latter congruence can be built up from solutions of $P(x) \equiv 0 \pmod{p}$ in a way illustrated by the following worked exercise.

Worked Exercise 4.10

Solve $x^3 + x + 5 \equiv 0 \pmod{27}$.

Solution

As $27 = 3^3$, we first solve the given congruence modulo 3. Trying $x = 0, 1$ and 2 , we find that

$$x^3 + x + 5 \equiv 0 \pmod{3}$$

has the unique solution $x \equiv 2 \pmod{3}$.

Moving up a power of 3, we next investigate

$$x^3 + x + 5 \equiv 0 \pmod{9}.$$

If a is a solution then $a^3 + a + 5$ is divisible by 9 (and therefore by 3), and so a is also a solution of $x^3 + x + 5 \equiv 0 \pmod{3}$. That is, $a \equiv 2 \pmod{3}$, and so the only possibilities are $a \equiv 2, 5$ or $8 \pmod{9}$.

Putting in these values:

$$2^3 + 2 + 5 = 15 \equiv 6 \pmod{9},$$

$$5^3 + 5 + 5 = 135 \equiv 0 \pmod{9},$$

$$(-1)^3 + (-1) + 5 = 3 \equiv 3 \pmod{9},$$

and so $x \equiv 5 \pmod{9}$ is the unique solution.

Moving up one more power of 3 and repeating the argument, any solution of

$$x^3 + x + 5 \equiv 0 \pmod{27}$$

must be a solution of $x^3 + x + 5 \equiv 0 \pmod{9}$ and hence must be congruent to 5 modulo 9. So we need to check only the three candidates $x \equiv 5, 14$ and $23 \pmod{27}$:

$$5^3 + 5 + 5 = 135 \equiv 0 \pmod{27},$$

$$14^3 + 14 + 5 = 2763 \equiv 9 \pmod{27},$$

$$(-4)^3 + (-4) + 5 = -63 \equiv 18 \pmod{27}.$$

We conclude that $x \equiv 5 \pmod{27}$ is the unique solution of the given congruence.

The strategy adopted in Worked Exercise 4.10 will work for a general congruence of this form. Each solution of congruence $P(x) \equiv 0 \pmod{p^k}$ is of the form $b + rp^{k-1}$, where b is a solution of the congruence $P(x) \equiv 0 \pmod{p^{k-1}}$ and $0 \leq r < p$.

Exercise 4.5

Solve the following congruences:

- (a) $x^2 + x - 7 \equiv 0 \pmod{25}$
 (b) $x^2 + 4x - 1 \equiv 0 \pmod{125}$.

Exercise 4.6

- (a) Show that $x = 1$ and $x = -2$ both satisfy

$$x^3 + 2x^2 + 6x + 5 \equiv 0 \pmod{7}.$$

Hence factorise $x^3 + 2x^2 + 6x + 5$ modulo 7 and find any further solutions of the congruence.

- (b) Solve the following polynomial congruences.

- (i) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{5}$
 (ii) $x^{12} - 1 \equiv 0 \pmod{7}$
 (iii) $x^5 - x^3 \equiv 0 \pmod{11}$
 (iv) $x^5 + x^3 \equiv 0 \pmod{17}$

- (c) Solve the following polynomial congruences.

- (i) $x^3 + 2x^2 + 3x + 9 \equiv 0 \pmod{35}$
 (ii) $x^3 + x^2 + 3x + 1 \equiv 0 \pmod{105}$
 (iii) $x^2 - 7x + 31 \equiv 0 \pmod{75}$

5 Fermat's and Wilson's Theorems revisited

This section is not assessed, and is for interest only.

The results of Fermat's Little Theorem and Wilson's Theorem are illustrated in the solutions of two well-known combinatorial problems.

Question 1 *Having enough beads to permit unlimited use of each of n colours, how many different necklaces consisting of p beads can be made, where p is prime?*

Do we understand what is being asked? We will assume that the necklaces are produced by first forming a string of p beads and then fusing the ends of the string. Our first step is therefore to count how many strings of p beads there are. Well, that's fairly straightforward. There are n choices for the first bead, n choices for the second bead, and so on. In all there are n^p strings.

Notice that, of the n^p strings, n strings consist of beads of one colour alone (one such for each colour). Hence there are $n^p - n$ strings involving at least two colours. As the single-colour necklaces are easily counted, we will

put these to one side and concentrate on the ones involving two or more colours.

As one must expect, the $n^p - n$ strings counted will not result in $n^p - n$ different necklaces being produced. For example, the five strings of beads involving colours A , B and C illustrated in Figure 5.1 all result in the same necklace.

The strings in this example are obtained from one another by removing the bead on the left and replacing it on the right of the string. We will call the operation of moving a bead from the left end to the right end a 'recycle'. Two strings that can be obtained from each other by a sequence of recycles clearly correspond to the same necklace.

The five strings in Figure 5.1 are different. But if we consider the string of four beads shown in Figure 5.2, we see that the second recycle produces a string with the same colour scheme, BABA, and that further recycles here produce just two different strings.

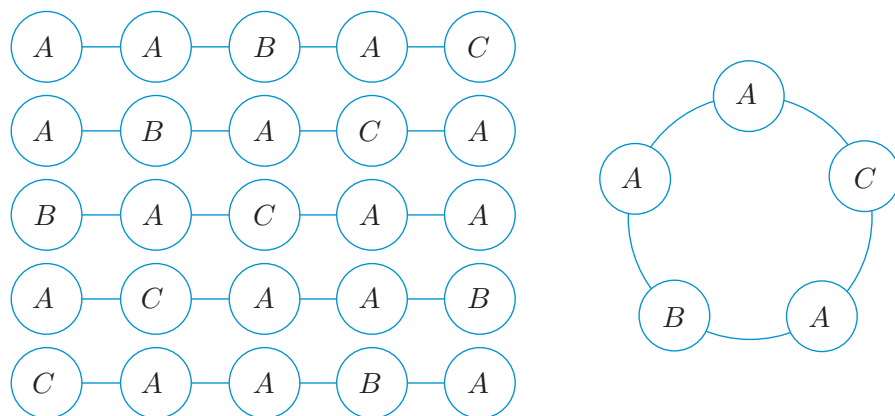


Figure 5.1 Five strings giving the same necklace



Figure 5.2 String of four beads

So we need to ask how many different strings can be obtained from a string of p beads by recycles. The obvious answer is p , since each of the p beads can occupy the left-end position, unless, as illustrated above for four beads, some fewer number of recycles restores the original colour scheme. We use the Division Algorithm to show that this cannot happen for a prime number of beads.

Let k be the least number of recycles that restores the colour scheme of a string of p beads, where $k > 1$ since we are ignoring strings of a single colour. Dividing p by k , there exist integers q and r such that

$$p = qk + r, \quad \text{where } 0 \leq r < k.$$

Now if k recycles restore the colour scheme then so too do $2k, 3k, \dots, qk$ recycles. Furthermore, p recycles certainly restore the colour scheme since each bead returns to its initial position. Therefore after the qk th recycle we have the original colour scheme and only a further r recycles are needed to restore it again. As k is the least number of recycles that can achieve this, we must conclude that $r = 0$. This in turn implies that k divides p and, since p is prime and $k > 1$, we must have $k = p$.

The outcome of this is that the $n^p - n$ strings involving two or more colours are partitioned into disjoint sets of p strings, each set consisting of strings that can be obtained from each other by a sequence of recycles. This means that p divides $n^p - n$, which is Fermat's Little Theorem.

One might be tempted to conclude from this that there are $\frac{n^p - n}{p}$ different necklaces involving two or more colours, and hence a grand total of $\frac{n^p - n}{p} + n$ different necklaces. Unfortunately there is a further complication to be taken into account. Consider the string shown in Figure 5.3.

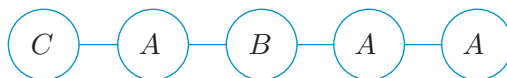


Figure 5.3 String of five beads

It is the first string of Figure 5.1 but with the order reversed (that is, turned over left to right). It gives rise to a further set of five strings that correspond to the same necklace (turned over) as shown in Figure 5.1. So there are really ten different strings that produce this necklace. In general, two different sets of p strings can give rise to the same necklace. We say 'can' because turning a string over does not always produce a new string, as illustrated by the string in Figure 5.4.



Figure 5.4 A symmetric string

Recycling gives five different strings, but if we then turn it over and recycle we get the same five again. To complete the task we have still to count these 'symmetric' strings. We leave you the task of completing Question 1 as a challenge. For the record, the number of necklaces is

$$\frac{n^p - n}{2p} + \frac{n^{(p+1)/2} - n}{2} + n.$$

Notice that as this is an integer value, the first term still incorporates FLT.

A similar problem leads to a demonstration of Wilson's Theorem.

Question 2 *How many stellated p -gons are there, where p is prime?*

A stellated n -gon is formed by placing n points symmetrically around the circumference of a circle and then joining these points with n straight line segments, crossings being allowed. For $n = 5$ there are twelve stellated pentagons, as shown in Figure 5.5.

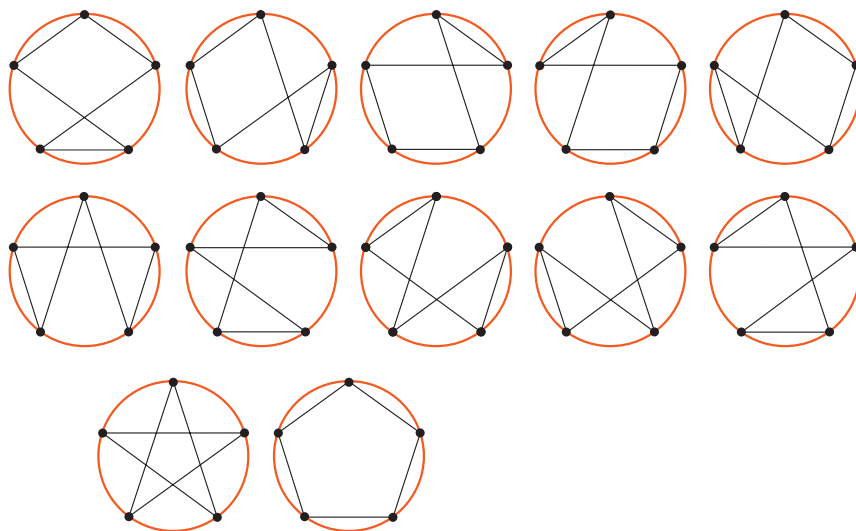


Figure 5.5 The twelve stellated pentagons

Notice that the five pentagons in the first row are congruent, being obtained from each other by rotations through $\frac{2\pi}{5}$. Similarly, the pentagons in the second row are congruent. The remaining two are the *regular* stellated pentagons, having rotation through $\frac{2\pi}{5}$ as a symmetry operation. Hence, if we classify stellated pentagons up to similarity (for we are not concerned about the size) there are two essentially different irregular ones plus the two regular ones.

In the same way we now want to count the number of different stellated p -gons, where $p > 2$ is prime. We will first count how many p -gons can be drawn (corresponding to the twelve pentagons) and then count how many of these are regular ones. The difference will give the irregular ones, which will fall into sets of p congruent p -gons, being obtained from each other by rotation through $\frac{2\pi}{p}$.

To count the total number of stellated p -gons, imagine starting at any point on the circle and drawing the p -gon. There are $p - 1$ choices for the first destination, then $p - 2$ choices for the second destination, and so on. In all, $(p - 1)!$ stellated p -gons can be drawn. But this has counted each p -gon twice, because one ordering of the p vertices visited and the reverse order give the same p -gon. Hence there are $\frac{(p - 1)!}{2}$ p -gons in all. (This agrees with the discovered 12 for the case $p = 5$.)

When p is not prime this construction will still draw a regular p -gon for each choice of k satisfying $\text{hcf}(k, p) = 1$.

The regular stellated p -gons are formed by choosing any k in the range $1 \leq k \leq p - 1$ and joining each point on the circle to the one k places round the circle clockwise from it. But again this counts each regular p -gon twice, because the choices of $k = r$ and $k = p - r$ will draw the same p -gon but visiting the points on the circle in reverse order. Hence there are $\frac{(p-1)}{2}$ regular stellated p -gons.

Finally, the $\frac{(p-1)!}{2} - \frac{(p-1)}{2}$ irregular stellated p -gons are partitioned into congruent sets of p each, as determined by rotation through $\frac{2\pi}{p}$. Hence the total number of different stellated p -gons is

$$\frac{(p-1)! - (p-1)}{2p} + \frac{p-1}{2}.$$

As this is an integer, the first term illustrates that p divides $(p-1)! - (p-1)$, or, in congruence notation, $(p-1)! \equiv -1 \pmod{p}$, which is Wilson's Theorem.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should:

- Understand the statement, proof and applications of Fermat's Little Theorem and its alternative formulation; recognise which formulation to use in a given scenario.
- Know the meaning of the term 'pseudoprime', and its connection with Fermat's Little Theorem.
- Be able to apply the Division Algorithm to compute decimal representations of fractions.
- Understand the meaning of and be able to compute the 'order' of an integer modulo p ; know what it means for the integer 10 to be a 'primitive root' of p ; recognise the connection with the decimal representation of rational numbers with prime denominator.
- Understand the statement and proof of Wilson's Theorem, and its converse; be able to use Wilson's Theorem to solve more complicated congruences.
- Know the definition of the 'degree' of a polynomial congruence.
- Understand the statement and proof of Lagrange's Theorem.
- Be able to use a variety of techniques to solve polynomial congruences with composite moduli.

Solutions to exercises

Solution to Exercise 1.1

- (a) Suppose that $a^p \equiv a \pmod{p}$ for all integers a . Then if $a \not\equiv 0 \pmod{p}$ we can cancel by a to obtain $a^{p-1} \equiv 1 \pmod{p}$, as required.
- (b) Suppose that $a^{p-1} \equiv 1 \pmod{p}$ for all a such that $a \not\equiv 0 \pmod{p}$. Then, multiplying by a , $a^p \equiv a \pmod{p}$ for all $a \not\equiv 0 \pmod{p}$. However, if $a \equiv 0 \pmod{p}$ then $a^p \equiv a \equiv 0 \pmod{p}$ and so $a^p \equiv a \pmod{p}$ for all integers a .

Solution to Exercise 1.2

- (a) (i) FLT tells us that $5^6 \equiv 1 \pmod{7}$. Therefore
- $$5^{20} \equiv (5^6)^3 \times 5^2 \equiv 1^3 \times 25 \equiv 25 \equiv 4 \pmod{7},$$
- and the remainder is 4.
- (ii) We first replace 37 with its least positive residue before using FLT:
- $$37 \equiv 3 \pmod{17}, \quad \text{and so} \quad 37^{37} \equiv 3^{37} \pmod{17}.$$
- Now FLT tells us that $3^{16} \equiv 1 \pmod{17}$ and so
- $$\begin{aligned} 37^{37} &\equiv 3^{37} \equiv (3^{16})^2 \times 3^5 \equiv 1^2 \times 3^5 \equiv 3^5 \pmod{17} \\ &\equiv 27 \times 9 \equiv 10 \times 9 = 90 \equiv 5 \pmod{17}, \end{aligned}$$
- and the remainder is 5.
- (b) If $x \equiv a^{p-2}b \pmod{p}$ then $ax \equiv a^{p-1}b \pmod{p}$. Now, since $\text{hcf}(a, p) = 1$, FLT gives $a^{p-1} \equiv 1 \pmod{p}$ and so $ax \equiv b \pmod{p}$, as claimed.

The congruence $5x \equiv 18 \pmod{19}$ has a unique solution modulo 19, which we now know is $x \equiv 5^{17} \times 18 \pmod{19}$. As $5^2 \equiv 6 \pmod{19}$, we have

$$\begin{aligned} x &\equiv 5^{17} \times 18 \pmod{19} \\ &= (5^2)^8 \times 5 \times 18 \pmod{19} \\ &\equiv (6^8 \times 5) \times (-1) \pmod{19} \\ &\equiv (-2)^4 \times (-5) \pmod{19}, \quad \text{since } 6^2 \equiv -2 \pmod{19}, \\ &\equiv (-3) \times (-5) \pmod{19} \\ &\equiv 15 \pmod{19}. \end{aligned}$$

Solution to Exercise 1.3

- (a) As $168 = 3 \times 7 \times 8$, to prove that 168 divides $a^6 - 1$, we will show that $a^6 \equiv 1 \pmod{3}$, $a^6 \equiv 1 \pmod{7}$ and $a^6 \equiv 1 \pmod{8}$. Since 3, 7 and 8 are pairwise coprime, it then follows from Theorem 1.6 of Chapter 3 that $a^6 \equiv 1 \pmod{168}$.

Given that $\text{hcf}(a, 42) = 1$, we know that $\text{hcf}(a, 2) = 1$, $\text{hcf}(a, 3) = 1$ and $\text{hcf}(a, 7) = 1$.

From $\text{hcf}(a, 7) = 1$, FLT gives $a^6 \equiv 1 \pmod{7}$.

From $\text{hcf}(a, 3) = 1$, FLT gives $a^2 \equiv 1 \pmod{3}$, whereupon

$$a^6 = (a^2)^3 \equiv 1^3 \equiv 1 \pmod{3}.$$

Finally, from $\text{hcf}(a, 2) = 1$ we have that a is odd. But

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8},$$

and so $a^2 \equiv 1 \pmod{8}$.

Therefore $a^6 = (a^2)^3 \equiv 1^3 \equiv 1 \pmod{8}$.

- (b) To focus on the units digit of a number amounts to consideration of the number modulo 10. So our task is to show that $a^5 \equiv a \pmod{10}$.

Now FLT gives $a^5 \equiv a \pmod{5}$. Moreover, $a^5 \equiv a \pmod{2}$, since a^5 is even if, and only if, a is even. As 2 and 5 are coprime it follows that $a^5 \equiv a \pmod{10}$.

What can we now say about $a^{100} \pmod{10}$?

$$a^{100} = (a^5)^{20} \equiv a^{20} = (a^5)^4 \equiv a^4 \pmod{10},$$

and so a^{100} and a^4 have the same units digit.

Solution to Exercise 1.4

- (a) $5^{12} \equiv 1 \pmod{13}$ by FLT.

$$5^{14} = 5^{12} \times 5^2 \equiv 1 \times 5^2 = 25 \equiv 12 \pmod{13}.$$

$$\begin{aligned} 1996^{14} &\equiv 7^{14} \pmod{13}, \quad \text{since } 1996 \equiv 7 \pmod{13}, \\ &\equiv 7^{12} \times 7^2 \equiv 1 \times 7^2 \pmod{13}, \quad \text{since } 7^{12} \equiv 1 \pmod{13} \text{ by FLT,} \\ &\equiv 10 \pmod{13}. \end{aligned}$$

- (b) (i) FLT gives $3^{16} \equiv 1 \pmod{17}$ and $5^{16} \equiv 1 \pmod{17}$. Therefore

$$3^{50} = (3^{16})^3 \times 3^2 \equiv 1^3 \times 9 \equiv 9 \pmod{17}$$

and

$$5^{50} = (5^{16})^3 \times 5^2 \equiv 1^3 \times 25 \equiv 8 \pmod{17}.$$

Hence $3^{50} + 5^{50} \equiv 9 + 8 \equiv 0 \pmod{17}$, and hence $3^{50} + 5^{50}$ is divisible by 17.

- (ii) As 97 is prime, FLT gives $2^{96} \equiv 3^{96} \equiv 1 \pmod{97}$. Therefore

$$\begin{aligned} 2^{100} + 3^{100} &= 2^{96} \times 2^4 + 3^{96} \times 3^4 \equiv 2^4 + 3^4 \pmod{97} \\ &= 16 + 81 \equiv 0 \pmod{97}. \end{aligned}$$

Hence $2^{100} + 3^{100}$ is divisible by 97.

Notice that as 8 is not prime we cannot use FLT.

- (c) $155 = 5 \times 31$, and FLT gives $7^4 \equiv 1 \pmod{5}$ and $7^{30} \equiv 1 \pmod{31}$.
Therefore

$$7^{154} = (7^{30})^5 \times 7^4 \equiv 7^4 \equiv 18^2 \equiv 14 \pmod{31}$$

and

$$7^{154} = (7^4)^{38} \times 7^2 \equiv 7^2 \equiv 4 \pmod{5}.$$

By the Chinese Remainder Theorem, the simultaneous congruences $x \equiv 14 \pmod{31}$ and $x \equiv 4 \pmod{5}$ have a unique solution modulo 155, which can be seen to be $x \equiv 14 \pmod{155}$. So the remainder on dividing 7^{154} by 155 is 14.

- (d) As $42 = 2 \times 3 \times 7$, we show that $a^7 \equiv a \pmod{2}$, $a^7 \equiv a \pmod{3}$ and $a^7 \equiv a \pmod{7}$, and then appeal to the corollary to Theorem 1.6 of Chapter 3.

Let a be *any* integer. For each of the primes $p = 2, 3$ and 7 we apply FLT in the form $a^p \equiv a \pmod{p}$.

$$p = 2: \quad a^7 = (a^2)^3 a \equiv a^3 a = (a^2)^2 \equiv a^2 \equiv a \pmod{2}$$

$$p = 3: \quad a^7 = (a^3)^2 a \equiv a^2 a = a^3 \equiv a \pmod{3}$$

$$p = 7: \quad a^7 \equiv a \pmod{7}$$

Hence, $a^7 \equiv a \pmod{42}$ for all integers a .

- (e) By FLT, $p^{q-1} \equiv 1 \pmod{q}$ and, since q divides q^{p-1} ,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q}.$$

Similarly

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p}.$$

Therefore, by Theorem 1.6 of Chapter 3, since $\text{hcf}(p, q) = 1$,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

- (f) For odd prime p we have $2^{p-1} \equiv 1 \pmod{p}$. Therefore

$$(p-1)2^{p-1} + 1 \equiv (p-1) \times 1 + 1 = p \equiv 0 \pmod{p}$$

and

$$(p-2)2^{p-2} + 1 = p \times 2^{p-2} - 2^{p-1} + 1 \equiv 0 - 1 + 1 \equiv 0 \pmod{p}.$$

There is no obvious reason why $(p-3)2^{p-3} + 1$ should be divisible by p , and indeed $p = 3$ gives a counter-example:

$$(3-3)2^{3-3} + 1 = 1 \not\equiv 0 \pmod{3}.$$

Solution to Exercise 2.1

$$\begin{aligned}
 \text{(a)} \quad & 1 = 0 \times 15 + 1 \\
 & 10 = 0 \times 15 + 10 \\
 & 100 = 6 \times 15 + 10 \\
 & 100 = 6 \times 15 + 10
 \end{aligned}$$

This last equation now repeats indefinitely. So $\frac{1}{15} = 0.0\langle 6 \rangle$.

$$\begin{aligned}
 \text{(b)} \quad & 1 = 0 \times 41 + 1 \\
 & 10 = 0 \times 41 + 10 \\
 & 100 = 2 \times 41 + 18 \\
 & 180 = 4 \times 41 + 16 \\
 & 160 = 3 \times 41 + 37 \\
 & 370 = 9 \times 41 + 1 \\
 & 10 = 0 \times 41 + 10
 \end{aligned}$$

The block of five equations now repeats indefinitely, and so $\frac{1}{41}$ has cycle length 5 and $\frac{1}{41} = 0.\langle 02439 \rangle$.

Solution to Exercise 2.2

FLT tells us that $10^{16} \equiv 1 \pmod{17}$ and so the straightforward approach is to check each smaller positive power of 10 in turn, looking for a least positive residue of 1. Going from one power to the next by multiplying by 10, the successive powers of 10 modulo 17 are

$$\begin{aligned}
 & 10, 100 \equiv 15, 150 \equiv 14, 140 \equiv 4, 40 \equiv 6, 60 \equiv 9, \\
 & 90 \equiv 5, 50 \equiv 16, 160 \equiv 7, 70 \equiv 2, 20 \equiv 3, \\
 & 30 \equiv 13, 130 \equiv 11, 110 \equiv 8, 80 \equiv 12, 120 \equiv 1.
 \end{aligned}$$

So the order of 10 modulo 17 is 16, and the cycle of $\frac{1}{17}$ has length 16.

Solution to Exercise 2.3

We know that $10^{60} \equiv 1 \pmod{61}$ and that c is the smallest positive integer for which $10^c \equiv 1 \pmod{61}$. Suppose that dividing 60 by c gives $60 = cq + r$, where $0 \leq r < c$.

Then $10^{60} = (10^c)^q \times 10^r \equiv 1^q \times 10^r \equiv 10^r \pmod{61}$. But $10^{60} \equiv 1 \pmod{61}$ so $10^r \equiv 1 \pmod{61}$. Therefore $r = 0$, for otherwise the order of 10 modulo 61 would be smaller than c . Hence c divides 60, as claimed.

Solution to Exercise 2.4

Notice that 10 is a primitive root of 17 (from Table 2.2, or from the length of the cycle of $\frac{1}{17}$ being 16 and Proposition 2.3).

$$2 = 0 \times 17 + 2$$

$$20 = 1 \times 17 + 3$$

$$30 = 1 \times 17 + 13$$

At this point we know that $\frac{2}{17}$ begins 0.11, which pinpoints the starting point in the cycle of $\frac{1}{17}$. Thus

$$\frac{2}{17} = 0.\langle 1176470588235294 \rangle.$$

Similarly

$$9 = 0 \times 17 + 9$$

$$90 = 5 \times 17 + 5$$

$$50 = 2 \times 17 + 16$$

shows that $\frac{9}{17}$ begins 0.52, and so we can deduce that

$$\frac{9}{17} = 0.\langle 5294117647058823 \rangle.$$

Solution to Exercise 2.5

(a) The system of equations for the decimal fraction of $\frac{1}{21}$ is as follows.

$$\begin{array}{l} 1 = 0 \times 21 + 1 \\ 10 = 0 \times 21 + 10 \\ 100 = 4 \times 21 + 16 \\ 160 = 7 \times 21 + 13 \\ 130 = 6 \times 21 + 4 \\ 40 = 1 \times 21 + 19 \\ 190 = 9 \times 21 + 1 \end{array}$$


The equations now cycle. So $\frac{1}{21} = 0.\langle 047619 \rangle$, having a cycle of length 6. As 6 is not a factor of $21 - 1$, Leibniz's claim is disproved.

(b) If $\frac{1}{p}$ has a cycle of length n then $10^n \equiv 1 \pmod{p}$. That is, p divides $10^n - 1$. Hence, $p < 10^n - 1$, confirming that the number of such p is finite.

(c) The prime decomposition of $10^4 - 1$ is

$$10^4 - 1 = 3^2 \times 11 \times 101.$$

If $\frac{1}{p}$ has a cycle of length 4 then $10^4 \equiv 1 \pmod{p}$ and so p must be a factor of $10^4 - 1$. These values are seen to be $p = 3, 11$ and 101 . For each of these p , the order of 10 modulo p is a factor of 4, namely 1, 2 or 4. Those p for which the order is less than 4 must satisfy $10^2 \equiv 1 \pmod{p}$, which happens only for p a factor of $10^2 - 1 = 99$; that is, $p = 3$ or 11 . We conclude that the only prime p for which $\frac{1}{p}$ has a cycle of length 4 is 101.

In the same way, those p for which $\frac{1}{p}$ has a cycle of length 6 are those prime factors of $10^6 - 1$ that are not factors of either $10^2 - 1$ or $10^3 - 1$, that is, any factor of $3^3 \times 7 \times 11 \times 13 \times 37$ that is not a factor of either $3^2 \times 11$ or $3^3 \times 37$. The only primes satisfying this condition are 7 and 13.

- (d) (i) If all cards return to their original position after n shuffles then

$$2^n x \equiv x \pmod{53}, \text{ for all } 1 \leq x \leq 52.$$

As $\text{hcf}(x, 53) = 1$ we may cancel x to obtain

$$2^n \equiv 1 \pmod{53}.$$

So n has to be a multiple of the order of 2 modulo 53, and indeed if n shuffles is the smallest number for which this occurs, n is the order of 2 modulo 53.

FLT tells us that $2^{52} \equiv 1 \pmod{53}$ so, by Proposition 2.4, the n we seek is a factor of 52. Checking $n = 2, 4, 13$ and 26 we find

$$2^2 = 4,$$

$$2^4 = 16,$$

$$2^{13} = 2^6 \times 2^6 \times 2 \equiv 11 \times 11 \times 2 \equiv 30 \pmod{53},$$

$$2^{26} = (2^{13})^2 \equiv 30^2 \equiv 52 \pmod{53}.$$

Therefore, as no smaller power of 2 is congruent to 1 modulo 53, the order of 2 modulo 53 is 52, and 52 shuffles are needed to restore the original order.

- (ii) When the number of cards in the pack goes up to 54, we have to find the smallest natural number n for which $2^n \equiv 1 \pmod{55}$. We note that 55 is not prime and so we are not able to start from $2^{54} \equiv 1 \pmod{55}$. However, noting that $55 = 5 \times 11$, FLT gives

$$2^4 \equiv 1 \pmod{5} \text{ and } 2^{10} \equiv 1 \pmod{11}.$$

As $\text{lcm}(4, 10) = 20$, we have

$$2^{20} = (2^4)^5 \equiv 1 \pmod{5} \text{ and } 2^{20} = (2^{10})^2 \equiv 1 \pmod{11}.$$

Since 5 and 11 are coprime, the corollary to Theorem 1.6 of Chapter 3 gives $2^{20} \equiv 1 \pmod{55}$, and we have one solution to our problem: 20 shuffles will restore the original order of the pack of 54 cards.

If c is the smallest positive integer such that $2^c \equiv 1 \pmod{55}$ then c must divide 20. Why? Suppose $20 = qc + r$, where $0 \leq r < c$. Then, as in the proof of Proposition 2.4,

$$a^{20} \equiv a^{qc+r} \equiv (a^c)^q \times a^r \equiv 1^q a^r \pmod{55}$$

showing that $a^r \equiv 1 \pmod{55}$ with $r < c$. Hence $r = 0$ and so c must divide 20.

The fact that 55 is not a prime does not affect the necessity for n to satisfy $2^n \equiv 1 \pmod{55}$, as $2^n x \equiv x \pmod{55}$ has to hold for all x , including $x = 1$.

However,

$$2^2 = 4,$$

$$2^4 = 16,$$

$$2^5 = 32,$$

$$2^{10} = 2^6 \times 2^4 \equiv 9 \times 16 = 144 \equiv 34 \pmod{55},$$

which shows that no smaller power of 2 is congruent to 1 modulo 55. So 20 is the least number of shuffles that restores the original order.

Solution to Exercise 3.1

- (a) Wilson's Theorem assures us that 19 divides $18! + 1$. For any prime $p < 19$, p divides $18!$ and so p cannot divide $18! + 1$. Hence 19 is the smallest prime dividing $18! + 1$.

- (b) Wilson's Theorem tells us that 31 divides $30! + 1$. Now

$$30! + 1 = 30 \times 29! + 1 \equiv (-1)29! + 1 = 1 - 29! \pmod{31},$$

and so 31 also divides $29! - 1$. Furthermore, 31 must be the smallest prime with this property because any prime $p < 31$ divides $29!$ and so cannot divide $29! - 1$.

Solution to Exercise 3.2

- (a) Worked Exercise 3.3 showed that for any prime $p = 4k + 1$, the congruence $x^2 + 1 \equiv 0 \pmod{4k + 1}$ has $x \equiv (2k)! \pmod{4k + 1}$ as a solution. For $k = 7$, the congruence $x^2 + 1 \equiv 0 \pmod{29}$ has solution $x \equiv 14! \pmod{29}$. Working modulo 29, we can simplify the calculation of $14!$ by pairing the terms appropriately:

$$\begin{aligned} 14! &= 1 \times (2 \times 14) \times (3 \times 10) \times (4 \times 7) \times (5 \times 6) \times (8 \times 11) \times (9 \times 13) \times 12 \\ &\equiv 1 \times (-1) \times 1 \times (-1) \times 1 \times 1 \times 1 \times 12 \pmod{29} \\ &\equiv 12 \pmod{29}. \end{aligned}$$

Since $(-x)^2 = x^2$, $x \equiv -12 \equiv 17 \pmod{29}$ is a second solution.

In fact $x \equiv 12, 17 \pmod{29}$ are the only solutions of this congruence, as you will see from the work of the next section.

- (b) Let us first illustrate the proof for the particular case $p = 11$. Working modulo 11, we have

$$2 \equiv -9, \quad 4 \equiv -7, \quad 6 \equiv -5, \quad 8 \equiv -3 \quad \text{and} \quad 10 \equiv -1.$$

Therefore,

$$\begin{aligned} -1 &\equiv 10! \pmod{11}, \quad \text{by Wilson's Theorem,} \\ &\equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \pmod{11} \\ &\equiv 1 \times 3 \times 5 \times 7 \times 9 \times (-9) \times (-7) \times (-5) \times (-3) \times (-1) \pmod{11} \\ &\equiv (-1)^5 \times 1^2 \times 3^2 \times 5^2 \times 7^2 \times 9^2 \pmod{11}. \end{aligned}$$

Multiplying through the final congruence by $(-1)^5$ gives

$$1^2 \times 3^2 \times 5^2 \times 7^2 \times 9^2 \equiv (-1)^6 \pmod{11},$$

This, of course, is not a very efficient method of solving the congruence. Its inclusion is to highlight the construction of Worked Exercise 3.3.

which is one of the required formulas. The second comes quickly from the observation that from $2 \equiv -9 \pmod{11}$ we have $2^2 \equiv 9^2 \pmod{11}$ and similarly

$$4^2 \equiv 7^2, 6^2 \equiv 5^2, 8^2 \equiv 3^2 \text{ and } 10^2 \equiv 1^2 \pmod{11}.$$

Substitution gives

$$2^2 \times 4^2 \times 6^2 \times 8^2 \times 10^2 \equiv (-1)^6 \pmod{11}.$$

The same argument works for any odd prime p :

$$2 \equiv -(p-2), 4 \equiv -(p-4), \dots, (p-1) \equiv -1 \pmod{p},$$

and so

$$\begin{aligned} -1 &\equiv (p-1)! \pmod{p} \\ &= (1 \times 3 \times 5 \times \dots \times (p-2)) \times (2 \times 4 \times 6 \times \dots \times (p-1)) \pmod{p} \\ &\equiv (1 \times 3 \times \dots \times (p-2)) \times (-(p-2) \times -(p-4) \times \dots \times (-1)) \pmod{p} \\ &\equiv (-1)^{(p-1)/2} \times 1^2 \times 3^2 \times \dots \times (p-2)^2 \pmod{p}. \end{aligned}$$

Multiplying by $(-1)^{(p-1)/2}$ gives

$$1^2 \times 3^2 \times \dots \times (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

For each k on the left of this congruence, we can replace k^2 with $(p-k)^2$ to get the alternative formula

$$2^2 \times 4^2 \times \dots \times (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Solution to Exercise 3.3

(a) The successive powers of 2 modulo 29 are given in the table below.

n	2^n	n	2^n	n	2^n	n	2^n
1	2	8	24	15	27	22	5
2	4	9	19	16	25	23	10
3	8	10	9	17	21	24	20
4	16	11	18	18	13	25	11
5	3	12	7	19	26	26	22
6	6	13	14	20	23	27	15
7	12	14	28	21	17	28	1

To get from one power to the next we just 'double modulo 29'.

Note that 2^n takes all 28 non-zero values modulo 29, confirming that the order of 2 modulo 29 is 28. Now, if $m+n=28$ then $2^m 2^n = 2^{m+n} = 2^{28} \equiv 1 \pmod{29}$. For example, taking $m=8$ and $n=20$,

$$2^8 \times 2^{20} \equiv 24 \times 23 \equiv (-5) \times (-6) = 30 \equiv 1 \pmod{29}.$$

In all there are 13 such pairs, 1 with 27, 2 with 26, ... and 13 with 15.

The value $n = 14$ (for which $2^{14} \equiv 28 \equiv -1 \pmod{29}$) is omitted because it pairs with itself. The pairs are

$$\begin{aligned} 2 \times 15 &\equiv 4 \times 22 \equiv 8 \times 11 \equiv 16 \times 20 \equiv 3 \times 10 \equiv 6 \times 5 \equiv 12 \times 17 \\ &\equiv 24 \times 23 \equiv 19 \times 26 \equiv 9 \times 13 \equiv 18 \times 21 \equiv 7 \times 25 \equiv 14 \times 27 \\ &\equiv 1 \pmod{29}. \end{aligned}$$

Multiplying all these thirteen pairs of numbers together gives

$$27! \equiv 1 \pmod{29},$$

and multiplying this through by 28 we reach

$$28! \equiv 28 \equiv -1 \pmod{29},$$

completing the illustration of the proof.

- (b) For any integer a and prime p , FLT gives $a^p \equiv a \pmod{p}$ and Wilson's Theorem gives $(p-1)! \equiv -1 \pmod{p}$. Therefore

$$a^p + a \times (p-1)! \equiv a + a \times (-1) \equiv 0 \pmod{p}$$

and

$$a + a^p \times (p-1)! \equiv a + a \times (-1) \equiv 0 \pmod{p}.$$

- (c) The result is certainly true for $p = 2$, and so we assume that p is odd. Since

$$1 + 2 + 3 + \cdots + (p-1) = \frac{p(p-1)}{2},$$

and p and $\frac{p-1}{2}$ are coprime integers, it suffices to show that

$$(p-1)! \equiv p-1 \pmod{p}$$

and

$$(p-1)! \equiv p-1 \pmod{\frac{p-1}{2}}.$$

The first of these is precisely Wilson's Theorem, and the second simply says that $0 \equiv 0$ since $\frac{p-1}{2}$ is a factor of $p-1$, and so

$$(p-1)! \equiv p-1 \pmod{\frac{p(p-1)}{2}}.$$

Solution to Exercise 4.1

- (a) Trying $x = 0, 1, 2, 3, 4$ and 5 , we find that $x^3 \equiv x \pmod{6}$ in each case and so the congruence $x^3 - x \equiv 0 \pmod{6}$ has six solutions, namely $x \equiv 0, 1, 2, 3, 4, 5 \pmod{6}$.
- (b) The straightforward approach is to test the result as x runs through a complete set of residues. However, recalling that $x^2 - 1 \equiv 0 \pmod{8}$ whenever x is odd, it follows that

$$x^3 - x = x(x^2 - 1) \equiv 0 \pmod{8} \text{ for } x \equiv 1, 3, 5, 7 \pmod{8}.$$

For x even, $0^3 - 0 \equiv 0$, $2^3 - 2 \equiv 6$, $4^3 - 4 \equiv 4$ and $6^3 - 6 \equiv 2 \pmod{8}$.

Hence there are five solutions in all, $x \equiv 0, 1, 3, 5, 7 \pmod{8}$.

See the solution to Exercise 1.3(a) in this chapter.

- (c) The values of the polynomial for a complete set of residues are given below.

x	$x^2 + x + 1 \pmod{7}$
0	1
1	3
2	$7 \equiv 0$
3	$13 \equiv 6$
4	$21 \equiv 0$
5	$31 \equiv 3$
6	$43 \equiv 1$

The numbers in the calculations here could have been kept smaller by using the set of least absolute residues modulo 7.

There are two solutions, namely $x \equiv 2, 4 \pmod{7}$.

- (d) First, we simplify the congruence by reducing the coefficients modulo 7 to get the equivalent congruence $2x^2 + 2x + 1 \equiv 0 \pmod{7}$. As x takes values 0, 1, 2, 3, 4, 5 and 6, $2x^2 + 2x + 1$ takes respective values $\pmod{7}$ 1, 5, 6, 4, 6, 5 and 1. Therefore this congruence has no solutions.

Solution to Exercise 4.2

- (a) This has degree 6. You may have noticed that this congruence can be reduced by FLT to an equivalent congruence of lower degree (0, in fact), but this is not immediately pertinent.
- (b) Since $10 \equiv 0 \pmod{5}$, the leading term modulo 5 is $3x$, and so the congruence has degree 1.
- (c) Since $15 \equiv 0 \pmod{5}$ and $-10 \equiv 0 \pmod{5}$, the leading term modulo 5 is the constant 2, and so the congruence has degree 0.

Solution to Exercise 4.3

- (a) Evaluating $x^2 + 4x - 4$ for $x = 0, \pm 1, \pm 2$ and ± 3 gives two solutions, $x \equiv -1$ and $x \equiv -3$. Pulling out the factor $(x + 1)$ corresponding to the first of these solutions,

$$x^2 + 4x - 4 \equiv (x + 1)(Ax + B) \pmod{7}$$

produces $A = 1$, $B = 3$ and the factorisation

$$x^2 + 4x - 4 \equiv (x + 1)(x + 3) \pmod{7}.$$

The second factor is the one expected, corresponding to the solution $x \equiv -3 \pmod{7}$.

- (b) By exhaustion, we find that $x^3 + 2x^2 + x + 3 \equiv 0 \pmod{7}$ has just the two solutions $x \equiv 1, 2 \pmod{7}$.

Pulling out the factor $(x - 1)$ gives

$$x^3 + 2x^2 + x + 3 \equiv (x - 1)(x^2 + 3x + 4) \pmod{7},$$

and then pulling out the factor $(x - 2)$ gives

$$\begin{aligned} x^3 + 2x^2 + x + 3 &\equiv (x - 1)(x - 2)(x + 5) \pmod{7} \\ &\equiv (x - 1)(x - 2)^2 \pmod{7}. \end{aligned}$$

The factors $x + 1$ and $x + 3$ could equally well be written as $x - 6$ and $x - 4$ respectively.

Solution to Exercise 4.4

As $80 = 2^4 \times 5$, we solve the congruences $x^2 - x + 4 \equiv 0 \pmod{16}$ and $x^2 - x + 4 \equiv 0 \pmod{5}$. By exhaustion,

$$x^2 - x + 4 \equiv 0 \pmod{16}$$

has solutions $x \equiv -3, 4 \pmod{16}$, and

$$x^2 - x + 4 \equiv 0 \pmod{5}$$

has the unique solution $x \equiv 3 \pmod{5}$.

Hence $x^2 - x + 4 \equiv 0 \pmod{80}$ has two solutions. By solving simultaneously,

$$x \equiv -3 \pmod{16} \text{ and } x \equiv 3 \pmod{5} \text{ yield } x \equiv 13 \pmod{80}$$

and

$$x \equiv 4 \pmod{16} \text{ and } x \equiv 3 \pmod{5} \text{ yield } x \equiv 68 \pmod{80}.$$

Solution to Exercise 4.5

- (a) By trial and error we find that $x^2 + x - 7 \equiv 0 \pmod{5}$ has solutions $x \equiv 1, 3 \pmod{5}$. So the only candidates for solution of $x^2 + x - 7 \equiv 0 \pmod{25}$ are:

$$\text{from } x \equiv 1 \pmod{5}, \quad x \equiv 1, 6, 11, 16 \text{ and } 21 \pmod{25}$$

and

$$\text{from } x \equiv 3 \pmod{5}, \quad x \equiv 3, 8, 13, 18 \text{ and } 23 \pmod{25}.$$

Of these,

$$11^2 + 11 - 7 = 125 \equiv 0 \pmod{25}$$

and

$$13^2 + 13 - 7 = 175 \equiv 0 \pmod{25}$$

are the only solutions. Hence $x^2 + x - 7 \equiv 0 \pmod{25}$ has solutions $x \equiv 11, 13 \pmod{25}$.

- (b) The congruence $x^2 + 4x - 1 \equiv 0 \pmod{5}$ has unique solution $x \equiv 3 \pmod{5}$. The candidates for solution of $x^2 + 4x - 1 \equiv 0 \pmod{25}$ are therefore $x \equiv 3, 8, 13, 18 \text{ and } 23 \pmod{25}$.

But

$$3^2 + 12 - 1 = 20 \equiv 20 \pmod{25},$$

$$8^2 + 32 - 1 = 95 \equiv 20 \pmod{25},$$

$$13^2 + 52 - 1 = 220 \equiv 20 \pmod{25},$$

$$(-7)^2 - 28 - 1 = 20 \equiv 20 \pmod{25},$$

$$(-2)^2 - 8 - 1 = -5 \equiv 20 \pmod{25}.$$

Hence $x^2 + 4x - 1 \equiv 0 \pmod{25}$ has no solutions, and from this $x^2 + 4x - 1 \equiv 0 \pmod{125}$ cannot have any solutions.

As 5 is prime, we know by Lagrange's Theorem there are at most two solutions; once we have found them we can stop.

This method still involves much computation, but whereas exhaustion would involve testing 25 values modulo 25, we have reduced this number to 10.

This time we have saved a lot of computation!

Solution to Exercise 4.6

(a) When $x = 1$,

$$x^3 + 2x^2 + 6x + 5 = 1 + 2 + 6 + 5 = 14 \equiv 0 \pmod{7},$$

and when $x = -2$,

$$x^3 + 2x^2 + 6x + 5 = -8 + 8 - 12 + 5 = -7 \equiv 0 \pmod{7}.$$

So both are solutions and it follows that

$$x^3 + 2x^2 + 6x + 5 \equiv (x - 1)(x + 2)(Ax + B) \pmod{7}.$$

A little algebra reveals that $A \equiv B \equiv 1 \pmod{7}$ and consequently $x + 1$ is also a factor. That gives a third solution, $x \equiv -1 \pmod{7}$. As Lagrange's Theorem guarantees that this congruence of degree 3 cannot have more than three solutions, we conclude that $x \equiv 1, -2, -1 \pmod{7}$ are all the solutions.

The least positive residue solutions are $x \equiv 1, 5, 6 \pmod{7}$.

(b) (i) Since $x \equiv 0 \pmod{5}$ is not a solution, we may assume that $\text{hcf}(5, x) = 1$ so that $x^4 \equiv 1 \pmod{5}$. Substituting this into the polynomial congruence produces

$$2(x^3 + x^2 + x + 1) \equiv 0 \pmod{5}.$$

Trial and error reveals that $x \equiv 2, 3$ and $4 \pmod{5}$ are the only three solutions.

(ii) $x^{12} - 1 = (x^6 - 1)(x^6 + 1) \equiv 0 \pmod{7}$

$x \equiv 0 \pmod{7}$ is not a solution, but for all other x we know from FLT that $x^6 - 1 \equiv 0 \pmod{7}$. So the congruence has six solutions, namely $x \equiv 1, 2, 3, 4, 5$ and $6 \pmod{7}$.

(iii) $x^5 - x^3 = x^3(x^2 - 1) \equiv 0 \pmod{11}$

$x^3 \equiv 0 \pmod{11}$ has the unique solution $x \equiv 0 \pmod{11}$, whilst $x^2 - 1 \equiv 0 \pmod{11}$ has at most two solutions (by Lagrange's Theorem), which can be seen to be $x \equiv \pm 1 \pmod{11}$. So there are three solutions, $x \equiv 0, 1$ and $10 \pmod{11}$.

(iv) $x^5 + x^3 = x^3(x^2 + 1) \equiv 0 \pmod{17}$

$x^3 \equiv 0 \pmod{17}$ has the unique solution $x \equiv 0 \pmod{17}$, whilst $x^2 + 1 \equiv 0 \pmod{17}$ has at most two solutions (by Lagrange's Theorem). Writing the latter in the equivalent form $x^2 \equiv -1 \pmod{17}$, the solutions are seen to be $x \equiv \pm 4 \pmod{17}$. So there are three solutions, $x \equiv 0, 4$ and $13 \pmod{17}$.

(c) (i) $x^3 + 2x^2 + 3x + 9 \equiv 0 \pmod{5 \times 7}$

We solve the congruence modulo 5 and modulo 7 and then look for simultaneous solutions.

$$x^3 + 2x^2 + 3x + 4 \equiv 0 \pmod{5}$$

has a unique solution (found by exhaustion) $x \equiv 1 \pmod{5}$.

$$x^3 + 2x^2 + 3x + 2 \equiv 0 \pmod{7}$$

has solutions $x \equiv 3, 6 \pmod{7}$.

If $x^3 \equiv 0 \pmod{11}$ then 11 divides x^3 . But that can happen only when 11 divides x .

$x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{7}$ if, and only if, $x \equiv 31 \pmod{35}$.

$x \equiv 1 \pmod{5}$ and $x \equiv 6 \pmod{7}$ if, and only if, $x \equiv 6 \pmod{35}$.

So there are two solutions, $x \equiv 6, 31 \pmod{35}$.

(ii) $x^3 + x^2 + 3x + 1 \equiv 0 \pmod{3 \times 5 \times 7}$

Proceeding as in part (i), we first solve the congruence for each of the moduli 3, 5 and 7. However, this congruence has no solutions modulo 5 (as discovered by trying each of the values 0, ± 1 , ± 2 for x). Hence the congruence has no solutions modulo 105.

(iii) As $75 = 3 \times 25$, we first solve $x^2 - 7x + 31 \equiv 0 \pmod{3}$, then solve $x^2 - 7x + 31 \equiv 0 \pmod{25}$ and finally find simultaneous solutions.

Working modulo 3:

$$x^2 - 7x + 31 \equiv x^2 - x + 1 \equiv 0 \pmod{3},$$

which is seen to have the unique solution $x \equiv 2 \pmod{3}$.

To solve $x^2 - 7x + 31 \equiv 0 \pmod{25}$ we first find the solutions, if any, modulo 5. As

$$x^2 - 7x + 31 \equiv x^2 - 2x + 1 = (x - 1)^2 \equiv 0 \pmod{5},$$

this has the unique solution $x \equiv 1 \pmod{5}$. It follows that the only candidates for solutions modulo 25 are

$$x \equiv 1, 6, 11, 16, 21 \pmod{25}.$$

A little arithmetic confirms that each of these five is a solution.

Hence the solutions of the original congruence are found by solving $x \equiv 2 \pmod{3}$ simultaneously with each of these five values modulo 25. Five solutions emerge:

$$x \equiv 11, 26, 41, 56, 71 \pmod{75}.$$

Index

- $3\mathbb{Z}$ 15
- $\langle \cdot \rangle$ 186
- $[r]$ 133
- $\equiv$ 128
- $\neq$ 128
- $\pi(x)$ 98
- $\tau(n)$ 81
- $|n|$ 16
- $b \mid a$ 30
- $b \nmid a$ 30

- angle brackets 186
- arithmetic progression 7
- arithmetic series 7

- basis for the induction 18
- Bertrand's Conjecture 85
- braces 15

- Cancellation Rule 137
- Carmichael numbers 185
- casting out nines 140
- Chinese Remainder Theorem 153
- complete set of residues 132
- composite 70
- congruence class 132
- congruent modulo n 128
- consecutive composite integers 95
- converse of Wilson's Theorem 196
- coprime 33
- Corollary to Euclid's Lemma for prime factors 75
- cycle 181, 187

- degree 94
- degree of a polynomial 94
- degree of a polynomial congruence 201
- degree of a polynomial modulo n 201
- density of primes 98
- Diophantine equation 44
- Dirichlet's Theorem 89
- divides 30
- divisibility 30
- divisibility by 11 141
- divisibility by 9 141
- Division Algorithm 27
- divisor 30

- 'equivalent to' symbol, $\Longleftrightarrow$ 138
- equivalent congruence 138
- Euclid's Lemma 35
- Euclid's Lemma for prime factors 75, 138
- Euclid's Theorem 84

- Euclidean Algorithm 41

- factor 30
- factorial 26
- factorising a polynomial congruence 203
- factors of an integer 79
- Fermat's Little Theorem 181
- Fermat's Little Theorem, an alternative formulation 182
- Fibonacci numbers 101
- Fibonacci numbers, coprimality of consecutive numbers 104
- Fibonacci numbers, divisibility property 106
- Fibonacci primes 102
- Fibonacci sequence 100
- FLT 182
- formula for $\tau(n)$ 82
- function τ 81
- Fundamental Theorem of Arithmetic 77

- $\gcd(a, b)$ 32
- geometric series 20
- Goldbach Conjecture, The 96
- greatest common divisor 32

- $\operatorname{hcf}(a, b)$ 32
- heptagonal numbers 11
- heptagonal-based pyramidal numbers 13
- hexagonal numbers 10
- highest common factor 32

- 'implies' symbol, $\implies$ 157
- incongruent modulo n 128
- induction hypothesis 18
- induction step 18
- integer 15
- integer combination 32
- integral polynomial 144

- $k!$ 26

- Lagrange's Theorem 202
- $\operatorname{lcm}(a, b)$ 38
- leading term of a polynomial 201
- least absolute residues 132
- least common multiple 38
- least positive residues 132
- length of a cycle 187
- $\operatorname{Li}(x)$ 98
- linear congruence 146
- linear Diophantine equation 44
- $\ln$ 98
- $\log$ 98
- logarithm 98

Index

- mathematical induction 18
- $\max\{a, b\}$ 81
- $\min\{a, b\}$ 80
- modulus 16
- multiple 30

- $\mathbb{N}$, the natural numbers 15
- non-negative integers 44
- non-terminating decimals 187
- number of solutions of a polynomial congruence 145

- octagonal numbers 11
- order of an integer 189

- $P(k, n)$, the n th k -gonal number 12
- pentagonal numbers 10
- perfect faro shuffle 194
- $\pi(x)$ 98
- polygonal numbers 11
- polynomial congruence 144, 199
- Poulet numbers 184
- prime 70
- prime decomposition 76
- prime decomposition of $\text{hcf}(m, n)$ 80
- prime decomposition of $\text{lcm}(m, n)$ 81
- Prime Number Theorem 98
- prime quartets 96
- prime triplets 96
- primes generated by polynomials 90
- primes in arithmetic progression 86
- primes of the form $4k + 3$ 88
- primitive root 190
- Principle of Induction 17
- Principle of Mathematical Induction 18
- Principle of Mathematical Induction (generalised) 21
- proper fraction 194
- properties of congruence 129

- pseudoprimes 184
- pyramidal numbers 12

- $Q(k, n)$, the n th k -gonal pyramidal number 14
- $\mathbb{Q}$, the rational numbers 15
- quadratic congruence 197

- $\mathbb{R}$, the real numbers 15
- rational numbers 15
- relatively prime 33
- repeating cycle 186
- residue class 132

- Second Principle of Mathematical Induction 23
- set 15
- sieve of Eratosthenes 72
- simultaneous linear congruences 153
- simultaneous solution 153
- size of the n th prime 84
- solution by exhaustion 146
- solutions of a polynomial congruence 199
- square number 8
- square-based pyramidal numbers 13

- T_n , the n th triangular number 7
- $\tau(n)$ 81
- terminating decimals 187
- triangle-based pyramidal numbers 12
- triangular numbers 7
- twin primes 94

- value of $\text{hcf}(n, p)$ 74

- Well-Ordering Principle 16
- Wilson's Theorem 195

- $\mathbb{Z}$, the integers 15
- $\mathbb{Z}_n$, the set of all residue classes modulo n 133

